PCT/GB 00 / 00752

The Patent Office

03 MARCH 2000

INVESTOR IN PEOPLE

09/936131

BEST AVAILABLE COPY

EJU

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 25 MAY 2000

WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears a correction, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Signed M. C...

Dated 29/3/2000

Patent Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

16DEC99 E4 9731-1 D03037
P01/7700 0.00-9929697.2

THE PATENT OFFICE
A
15 DEC 1999
RECEIVED BY FAX

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

Request for grant of a patent

(see the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1.	Your reference	RBF/P518
2.	Patent application number	9929697.2 — 15 DEC 1999
3.	Full name, address and postcode of the or of each applicant *(underline all surnames)*	Hewlett Packard ~~Limited~~ Company 3000 Hanover Street Palo Alto California 94304 USA
	Patents ADP number *(if you know it)*	4965880004
	If the application is a corporate body, give the country/state of its incorporation	
4.	Title of the invention	Smartcard User Interface for Trusted Computing Platform
5.	Name of your agent *(if you have one)* "Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	Franks & Co 352 Omega Court Cemetery Road Sheffield S11 8FT
	Patents ADP number *(if you know it)*	07451917001

6.	If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number	Country	Priority application number *(if you know it)*	Date of filing *(day/month/year)*

7.	If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing *(day/month/year)*

8. Is a statement of inventorship and or right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant or
c) any named applicant is a corporate body
(See note (d))

Received 15-12-99 21:22 From-44 114 268 0831 To-THE PATENT OFFICE Page 03

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	43
Claim(s)	11
Abstract	01
Drawing(s)	17

PML

10. If you are also filing any of the following, state how many against each item.

Priority documents	00
Translations of priority documents	00
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	00
Request for preliminary examination and search *(Patents Form 9/77)*	00
Request for substantive examination *(Patents Form 10/77)*	00
Any other documents *(please specify)*	00

11. I/We request the grant of a patent on the basis of this application.

Signature [illegible] Date 15 Dec 1999

Franks & Co

12. Name and daytime telephone number of person to contact in the United Kingdom **Robert Benjamin Franks Telephone: 0114 268 0929**

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patent s Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patents Office.*

SMARTCARD USER INTERFACE FOR TRUSTED COMPUTING PLATFORM

Field of the Invention

The present invention relates to the field of computers, and particularly, although not exclusively, to a computing entity which can be placed into a trusted state, and a method of operating the computing entity such that a user of the entity is confident that the computing entity is in the trusted state.

Background to the Invention

Conventional prior art mass market computing platforms include the well-known personal computer (PC) and competing products such as the Apple Macintosh™, and a proliferation of known palm-top and laptop personal computers. Generally, markets for such machines fall into two categories, these being domestic or consumer, and corporate. A general requirement for a computing platform for domestic or consumer use is a relatively high processing power, Internet access features, and multi-media features for handling computer games. For this type of computing platform, the Microsoft Windows® '95 and '98 operating system products and Intel processors dominate the market.

On the other hand, for business use in many applications, a server platform provides centralized data storage, and application functionality for a plurality of client stations. For business use, key criteria are reliability, networking features, and security features. For such platforms, the Microsoft Windows NT 4.0™ operating system is common, as well as the Unix™ operating system.

With the increase in commercial activity transacted over the Internet, known as "e-commerce", there has been much interest in the prior art in enabling data transactions between computing platforms over the Internet of both domestic and commercial types. A fundamental issue in acceptance of such systems is the

Received 15-12-99 21:22 From-44 114 268 0931 To-THE PATENT OFFICE Page 05

one of trust between interacting computer platforms for the making of such transactions.

There have been several prior art schemes which are aimed at increasing the security and trustworthiness of computer platforms. Predominantly, these rely upon adding in security features at the application level, that is to say the security features are not inherently embedded in the kernel of operating systems, and are not built in to the fundamental hardware components of the computing platform. Portable computer devices have already appeared on the market which include a smartcard, which contains data specific to a user, which is input into a smartcard reader on the computer. Presently, such smartcards are at the level of being add-on extras to conventional personal computers, and in some cases are integrated into a casing of a known computer. Although these prior art schemes go some way to improving the security of computer platforms, the levels of security and trustworthiness gained by prior art schemes may be considered insufficient to enable widespread application of automated transactions between computer platforms. For businesses to expose significant value transactions to electronic commerce on a widespread scale, they require confidence in the trustworthiness of the underlying technology.

Prior art computing platforms have several problems which stand in the way of increasing their inherent security:

- The operating status of a computer platform and the status of the data within the platform is dynamic and difficult to predict. It is difficult to determine whether a computer platform is operating correctly because the state of the computer platform and data on the platform is constantly changing and the computer platform itself may be dynamically changing.

- From a security point of view, commercial computer platforms, in particular client platforms, are often deployed in environments which are vulnerable to unauthorized modification. The main areas of vulnerability include modification by software loaded by a user, or via a network connection. Particularly, but not exclusively, conventional computer platforms may be vulnerable to attack by virus programs, with varying degrees of hostility.

- Computer platforms may be upgraded or their capabilities may be extended or restricted by physical modification, i.e. addition or deletion of components such as hard disk drives, peripheral drivers and the like.

It is known to provide security features for computer systems, which are embedded in operating software. These security features are primarily aimed at providing division of information within a community of users of a local system. In the known Microsoft Windows NT™ 4.0 operating system, there exists a monitoring facility called a "system log event viewer" in which a log of events occurring within the platform is recorded into an event log data file which can be inspected by a system administrator using the windows NT operating system software. This facility goes some way to enabling a system administrator to security monitor pre-selected events. The event logging function in the Windows NT™ 4.0 operating system provides system monitoring.

In terms of overall security of a computer platform, a purely software based system is vulnerable to attack, for example by viruses of which there are thousands of different varieties. Several proprietary virus finding and correcting applications are known, for example the Dr Solomons ™ virus toolkit program or Norton ™ anti-virus kit. The Microsoft Windows NT™ 4.0 software includes a virus guard software, which is preset to look for known viruses. However, virus strains are developing continuously, and the virus guard software will not give reliable protection against newer unknown viruses. New strains of virus are being

developed and released into the computing and internet environment on an ongoing basis.

Prior art monitoring systems for computer entities focus on network monitoring functions, where an administrator uses network management software to monitor performance of a plurality of networked computers. In these known systems, trust in the system does not reside at the level of individual trust of each hardware unit of each computer platform in a system, but relies on a network administrator monitoring each computer in the network. Prior art systems cannot verify operation of remote computers running different operating systems on different networks, for example as accessed over the internet.

In known systems there is difficulty in establishing trust between a user of a computing platform and the computing platform.

Summary of the Invention

One object of the present invention is to provide a computing entity in which a user can have a high degree of confidence that the computing entity has not been corrupted by an external influence, and is operating in a predictable and known manner.

Another object of the present invention is to simplify a task of a user of a computing entity judging whether the trustworthiness of the computing entity is sufficient to perform a particular task or set of tasks or type of task required by the user.

In the specific embodiments, the user is provided with a trusted token device which is portable and separable from a computer entity. The token device is trusted by the user to verify that a computer entity which the user wishes to use is trustworthy. In the general case, the token device is not restricted to verifying

the trustworthiness of one particular computer entity, but is generic to operate with any one or more of a plurality of computer entities.

According to first aspect of the present invention there is provided a system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

Said token device may receive a detailed response to said integrity challenge, and process said integrity response to interpret said integrity response.

The system may further comprise a third party server, wherein a response to said integrity challenge is sent to said third party server.

Said monitoring component may send a detailed integrity response to said third party server if requested in the integrity challenge by said token device.

Said monitoring component may report a detailed integrity response to said token device, and said token device may send said integrity response to said third party server, if it requires the third party server to help interpret said detailed integrity response.

Said third party server may simplify said integrity response to a form in which said token device can interpret said integrity response.

Said third party server may send said simplified integrity response to said token device.

The system may further operate the steps of adding a digital signature data to said simplified integrity response, said digital signature data authenticating said third party server to said token device.

Said token device may be requested to take an action. Alternatively, said token device may request to take an action.

In one mode of operation, the token device may send image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform may display said image data.

Preferably said monitoring component is capable of establishing an identity of itself.

Preferably the system further comprises an interface means for interfacing between said monitoring component and said token device.

Preferably said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

A said specific action may comprise authorising said computing platform to undertake a transaction on behalf of a user of said system.

According to a second aspect of the present invention there is provided a system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means:

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein said token device sends an integrity challenge to said monitoring component;

said monitoring component generates a response to said integrity challenge;

If said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and

said computer platform displays said verification data on a visual display screen.

According to a third aspect of the present invention there is provided a computing entity comprising:

a computing platform having a first data processor and first data storage means;

a monitoring component having a second data processor and second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself.

interface means for communicating with a token device, said interface means communicating with said monitoring component,

wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

Preferably on communication between said token device and said interface means, said monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

Said interface means is resident substantially wholly within said monitoring component in a best mode implementation. In an alternative implementation, said interface means may comprise said computer platform.

Said interface means preferably comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0.

Said monitoring component may comprise a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means.

Said interface means may be configured to send and receive data according to a pro-active protocol.

According to a fourth aspect of the present invention there is provided a method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and

said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

Said monitoring operation may comprise the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform;

said monitoring component being able to report a set of certified reference data together with said data checks.

Said certified reference data may include a set of metrics to be expected when measuring particular components of said computing platform, and may include digital signature data identifying an entity that certifies said reference data.

Preferably said step of reporting verification of said monitoring operation comprises sending a confirmation signal to a token device said confirmation signal describing a result of said monitoring operation.

Preferably said result message is transmitted by said interface to a token device external of said computing entity.

A result of said monitoring operation may be reported by generating a visual display of confirmation data.

The method may further comprise the steps of:

adding a digital signature data to said result message, said digital signature data identifying said monitoring component;

transmitting said result message and said digital signature data from said interface.

According to a fifth aspect of the present invention there is provided a method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a said token device;

in response to said request for access to functionality, said token device generating a request signal requesting a verification data from said monitoring component;

in response to said request for verification, said monitoring component reports a result message to said token device, said result message describing a result of a monitoring operation;

by receipt of a satisfactory said result message, said token device offers said functionality to said application.

The method may further comprise a response to said integrity challenge being sent to said third party server.

Said monitoring component may send a detailed integrity response to said third party server if requested in the integrity challenge by said token device.

The said monitoring component may report a detailed integrity response to said token device, and said token device may send said integrity response to said third party server, if it requires the third party server to help interpret said detailed integrity response.

Said third party server may simplify said integrity response to a form in which said token device can interpret said integrity response.

Said third party server may send said simplified integrity response to said token device.

The method may further operate the step of adding a digital signature data to said simplified integrity response, said digital signature data authenticating said third party server to said token device.

Said token device may be requested to take an action. Alternatively, said token device may request to take an action.

According to a sixth aspect of the present invention there is provided a method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means, and a monitoring component comprising a second processor and second memory means, by means of a token device, said token device comprising a third data processor and a third memory means, said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform;

said token device receiving a poll signal from said computer platform;

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

According to a seventh aspect of the present invention there is provided a token device for verifying a status of a computing entity, said token device comprising:

a data storage device; and

means for communicating with a computing entity;

wherein said data storage device is configured to store a status request message for requesting a status data from said computing entity.

Said token device may further comprise a data processor.

Said token device may be configured to be responsive to a poll signal operating in accordance with PC/SC specification 1.0, said token device may be capable of initiating a command to be handled by a software stack on the computer entity in response to said poll signal according to a proactive protocol.

According to an eighth aspect of the present invention there is provided a method of verifying a status of a computing entity, by means of a token device provided external of said computing entity, said method comprising the steps of:

said token device receiving a poll signal;

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity; and

said token device receiving a result message, said result message describing the result of said verification.

The method may further comprise sending a response to said integrity challenge to said third party server.

Said monitoring component may send a detailed integrity response to said third party server if requested in the integrity challenge by said token device.

Said monitoring component may report a detailed integrity response to said token device, and said token device may send said integrity response to said third party server, if it requires the third party server to help interpret said detailed integrity response.

Said third party server may simplify said integrity response to a form in which said token device can interpret said integrity response.

Said third party server may send said simplified integrity response to said token device.

The system may further operate the step of adding a digital signature data to said simplified integrity response, said digital signature data authenticating said third party server to said token device.

Said token device may be requested to take an action. Alternatively, said token device may request to take an action.

The invention includes a method by which a token device can obtain verification of a state of a computing platform by using a monitoring component,

said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself , and establishing a report of said at least one data check; and

wherein said token device has data processing capability and behaves in an expected manner;

said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability

wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform.

The invention includes a token device comprising a data processor and a memory device, said token device configured to perform at least one data processing or signaling function:

wherein said token device operates to:

receive an integrity check data from an external source;

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function; and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function.

Brief Description of the Drawings

For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

Fig. 1 illustrates schematically a computer entity according to a first specific embodiment of the present invention;

Fig. 2 illustrates schematically connectivity of selected components of the computer entity of Fig. 1;

Fig. 3 illustrates schematically a hardware architecture of components of the computer entity of Fig. 1;

Fig. 4 illustrates schematically an architecture of a trusted component comprising the computer entity of Fig. 1;

Fig. 5 illustrates schematically a logical architecture of the computer entity, divided into a monitored user space resident on a computer platform and a trusted space resident on the trusted component;

Fig. 6 illustrates schematically components of a smartcard token device for insertion into a smartcard reader of the computing entity;

Fig. 7 illustrates schematically a set of process steps carried out by a smartcard and computing entity according to a first use model;

Fig. 8 illustrates schematically a second mode of operation of the computing entity and smartcard in which an application requests authorization from the smartcard;

Fig. 9 illustrates schematically communication between the smartcard and an interface module comprising the computing entity;

Fig. 10 illustrates schematically a third mode of operation of the smartcard and computing entity in which the smartcard authenticates operation of the computing entity;

Fig. 11 illustrates schematically a computing system comprising a computing entity, a token device, and a remote trusted server, in which the token device delegates computation of a crypted integrity metrics to the trusted server in order to verify information received from a trusted component within a computing entity;

Fig. 12 illustrates schematically a mode of operation of the system of Fig. 11 in which integrity metric data is sent from a trusted component to a token device and the token device then sends the data to a trusted server for data processing according to fourth mode of operation;

Fig. 13 illustrates schematically an operation of the system of Fig. 11 in which the smartcard verifies the trustworthiness of a computing entity, by obtaining a certificate from a trusted third party according to a fifth mode of operation;

Fig. 14 illustrates schematically operation of the system of Fig. 11 from the point of view of a smartcard, for receiving a digital certificate and digital signature data from a trusted component according to a sixth mode of operation;

Fig. 15 illustrates schematically a third specific embodiment implementation of a system according to the present invention in which conventional PCSC technology is used to communicate with a smartcard, and in which the smartcard is able to give authorization for a transaction to a prior art application program, which operates through a subsystem interface to a trusted component;

Fig. 16 illustrates schematically operation of the embodiment shown in Fig. 15 enabling a smartcard to allow authorization for a transaction after having received confirmation of a trustworthy state of a computer entity with which it is co-operating.

Detailed Description of the Best Mode for Carrying Out the Invention

There will now be described by way of example the best mode contemplated by the inventors for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

Specific implementations of the present invention comprise a computer platform having a processing means and a memory means, and a monitoring component which is physically associated with the computer platform, and known herein after as a "trusted component" which monitors operation of the computer platform by collecting metrics data from the computer platform, and which is capable of verifying to other entities interacting with the computer platform, the correct functioning of the computer platform. A token device which may be personal to a human user of computer platform interacts with a trusted

component associated with the computer platform to verify to the human user the trustworthiness of the computer platform.

A user of a computing entity established a level of trust with the computer entity by use of such a trusted token device. The trusted token device is a personal and portable device having a data processing capability and in which the user has a high level of confidence. The trusted token device may perform the functions of:

- verifying a correct operation of a computing platform in a manner which is readily apparent to the user, for example by audio or visual display;

- challenging a monitoring component to provide evidence of a correct operation of a computer platform with which the monitoring component is associated; and

- establishing a level of interaction of the token device with a computing platform, depending on whether a monitoring component has provided satisfactory evidence of a correct operation of the computing entity, and withholding specific interactions with the computer entity if such evidence of correct operation is not received by the token device.

The token device may be requested to take an action, for example by an application resident on the computing platform, or by remote application, or alternatively the token device may initiate an action itself.

In this specification, the term "trusted" when used in relation to a physical or logical component, is used to mean that the physical or logical component always behaves in an expected manner. The behavior of that component is predictable

and known. Trusted components have a high degree of resistance to unauthorized modification.

In this specification, the term 'computer entity' is used to describe a computer platform and a monitoring component.

In this specification, the term "computer platform" is used to refer to at least one data processor and at least one data storage means, usually but not essentially with associated communications facilities e.g. a plurality of drivers, associated applications and data files, and which may be capable of interacting with external entities e.g. a user or another computer platform, for example by means of connection to the internet, connection to an external network, or by having an input port capable of receiving data stored on a data storage medium, e.g. a CD ROM, floppy disk, ribbon tape or the like. The term "computer platform" encompasses the main data processing and storage facility of a computer entity.

By use of a trusted component in each computing entity, there is enabled a level of trust between different computing platforms. It is possible to query such a platform about its state, and to compare it to a trusted state, either remotely, or through a monitor on the computer entity. The information gathered by such a query is provided by the computing entity's trusted component which monitors the various parameters of the platform. Information provided by the trusted component can be authenticated by cryptographic authentication, and can be trusted.

The presence of the trusted component makes it possible for a piece of third party software, either remote or local to the computing entity to communicate with the computing entity in order to obtain proof of its authenticity and identity and to retrieve measured integrity metrics of that computing entity. The third party

software can then compare the metrics obtained from the trusted component against expected metrics in order to determine whether a state of the queried computing entity is appropriate for the interactions which the third party software item seeks to make with the computing entity, for example commercial transaction processes.

This type of integrity verification between computing entities works well in the context of third party software communicating with a computing entity's trusted component, but does not provide a means for a human user to gain a level of trustworthy interaction with his or her computing entity, or any other computing entity which that person may interact with by means of a user interface.

In the best mode implementation described herein, a trusted token device is used by a user to interrogate a computing entity's trusted component and to report to the user on the state of the computing entity, as verified by the trusted component.

Referring to Fig. 1 herein, there is illustrated schematically one example of a computer entity according to a first specific implementation of the present invention. Referring to Fig. 2 of the accompanying drawings, there is illustrated schematically physical connectivity of some of the components of the computer entity of Fig. 1. Referring to Fig. 3 herein, there is illustrated schematically an architecture of the computer entity of Figs. 1 and 2, showing physical connectivity of components of the entity.

In general, in the best mode described herein, a computer entity comprises a computer platform consisting of a first data processor, and a first memory means, together with a trusted component which verifies the integrity and correct functioning of the computing platform. The trusted component comprises a

second data processor and a second memory means, which are physically and logically distinct from the first data processor and first memory means. The computer entity is provided with a smartcard reader port into which a user's smartcard can be inserted. The smartcard performs the function of being a 'trusted token' which a human user uses as a tool for verifying the integrity of a computing entity which is being used. Having verified the trustworthiness of the computing entity, by means of the user's trusted token device having corresponded with a trusted component in the computer entity, the user can then have confidence of the trustworthiness of the computing platform of the computing entity, and therefore have a higher level of confidence in using said computer platform.

In the example shown in Figs. 1 to 3 herein, the trusted computer entity is shown in the form of a personal computer suitable for domestic use or business use. However, it will be understood by those skilled in the art that this is just one specific embodiment of the invention, and other embodiments of the invention may take the form of a palmtop computer, a laptop computer, a server-type computer, a mobile phone-type computer, or the like and the invention is limited only by the scope of the claims herein. In the best mode example described herein, the computer entity comprises a display monitor 100; a keyboard data entry means 101; a casing 102 comprising a motherboard on which is mounted a data processor; one or more data storage means e.g. hard disk drives; a dynamic random access memory; various input and output ports (not illustrated in Fig. 1); a smartcard reader 103 for accepting a user's smartcard 105; a pointing device, e.g. a mouse or trackball device 106; and a trusted component for monitoring operations of the computing entity.

The user's smartcard 105 itself does not comprise the computing entity, but is a separate token device which interacts with the computing entity via the smartcard reader port 103. A user may have several different smartcards issued

by several different vendors or service providers, and may gain access to the internet or a plurality of network computers from any one of a plurality of computing entities as described herein, which are provided with a trusted component and smartcard reader. A user's trust in the individual computing entity to which s/he is using is derived from the interaction between the user's trusted smartcard token and the trusted component of the computing entity. The user relies on their trusted smartcard token to verify the trustworthiness of the trusted component.

Referring to Fig. 2 herein, there are illustrated some of the components comprising the trusted computer entity, including keyboard 101, which incorporates confirmation key 104 and smartcard reader 103; a main motherboard 200 on which is mounted first data processor 201 and trusted component 202, an example of a hard disc drive 203, and monitor 100. Additional components of the trusted computer entity include an internal frame to the casing 102, housing one or more local area network (LAN) ports, one or more modem ports, one or more power supplies, cooling fans and the like (not shown in Fig. 2).

In the best mode herein, as illustrated in Fig. 3 herein, main motherboard 200 is manufactured comprising a first data processor 201; and preferably a permanently fixed trusted component 202; a local memory device 300 to the first data processor, the local memory device being a fast access memory area, e.g. a random access memory; a BIOS memory area 301; smartcard interface 305; a plurality of control lines 302; a plurality of address lines 303; a confirmation key interface 306; and a data bus 304 connecting the processor 201, trusted component 202, memory area 300, a BIOS memory component 301 and smartcard interface 305.

External to the motherboard and connected thereto by data bus 304 are provided the one or more hard disk drive memory devices 203, keyboard data entry device 101, pointing device 106, e.g. a mouse, trackball device or the like; monitor device 100; smartcard reader device 103 for accepting a smartcard device as described previously; the disk drive(s), keyboard, monitor, and pointing device being able to communicate with processor 201 via said data bus 304; and one or more peripheral devices 307, 308, for example a modem, printer scanner or other known peripheral device.

In a best mode implementation, trusted component 202 is positioned logically and physically between monitor 100 and processor 201 of the computing platform, so that the trusted component 202 has direct control over the views displayed on monitor 100 which cannot be interfered with by processor 201.

The trusted component lends its identity and trusted processes to the computer platform and the trusted component has those properties by virtue of its tamper-resistance, resistance to forgery, and resistance to counterfeiting. Only selected entities with appropriate authentication mechanisms are able to influence the processes running inside the trusted component. Neither a user of the trusted computer entity, nor anyone or any entity connected via a network to the computer entity may access or interfere with the processes running inside the trusted component. The trusted component has the property of being "inviolate".

In the best mode, smartcard reader 103 is wired directly to smartcard interface 305 on the motherboard and does not connect directly to data bus 304. Alternatively, smartcard reader 103 may be connected directly to data bus 304. On each individual smartcard may be stored a corresponding respective image data which is different for each smartcard. For user interactions with the trusted component, e.g. for a dialogue box monitor display generated by the trusted component, the trusted component may take the image data from the user's

smartcard, and uses this as a background to the dialogue box displayed on the monitor 100. Thus, the user has confidence that the dialogue box displayed on the monitor 100 is generated by the trusted component. The image data is preferably easily recognizable by a human being in a manner such that any forgeries would be immediately apparent visually to a user. For example, the image data may comprise a photograph of a user. The image data on the smartcard may be unique to a person using the smartcard.

Referring to Fig. 4 herein, there is illustrated schematically an internal architecture of trusted component 202. The trusted component comprises a processor 400, a volatile memory area 401; a non-volatile memory area 402; a memory area storing native code 403; and a memory area storing one or a plurality of cryptographic functions, 404, the non-volatile memory 402, native code memory 403 and cryptographic memory 404 collectively comprising the second memory means herein before referred to. The trusted component is capable of storing programs and algorithms for interfacing with applications on the computer platform, or a remote computer platform; a verification interface 510 for pro-actively making integrity check measurements on the computer platforms; and an application interface 512.

Referring to Fig. 5 herein, there is illustrated schematically a logical architecture of the computer entity 500. The logical architecture has a same basic division between the computer platform, and the trusted component, as is present with the physical architecture described in Figs. 1 to 3 herein. That is to say, the trusted component is logically distinct from the computer platform to which it is physically related. The computer entity comprises a user space 501 being a logical space which is physically resident on the computer platform (the first processor and first data storage means) and a trusted component space 502 being a logical space which is physically resident on the trusted component 202. In the user space 501 are one or a plurality of drivers 503, one or a plurality of

applications programs 504, a file storage area 505; smartcard reader 103; smartcard interface 305; and a software agent 506 which can perform operations in the user space and report back to trusted component 202. The trusted component space is a logical area based upon and physically resident in the trusted component, supported by the second data processor and second memory area of the trusted component. Monitor 100 receives images directly from the trusted component space 502. External to the computer entity are external communications networks e.g. the Internet 507, and various local area networks, wide area networks 508 which are connected to the user space via the drivers 503 which may include one or more modem ports. External user smartcard 509 inputs into smartcard reader 103 in the user space.

Referring to Fig. 6 herein, there is illustrated schematically main components of a smartcard configured for use as a trusted token device. The smartcard comprises a base portion 600, for example of plastics sheet material; a read only memory area 601; a programmable memory area 602; a processor 603, and an array of connection contacts 604 by means of which the processor, and memory areas can connect with smartcard reader 103 of the computing entity for communication between the smartcard and the computing entity. In the general case, the smartcard does not contain its own power supply, electrical power to the memory areas and processor of the smartcard being provided by the computing entity via the smartcard reader 103.

Several different implementations of the invention are possible. In a best mode first implementation, the monitor 100 may be driven directly by a monitor subsystem contained within the trusted component itself. In this embodiment, in the trusted component space are resident the trusted component itself, and displays generated by the trusted component on monitor 100.

In the best mode first implementation, the subsystem 511 resides on the computer platform, and provides interfaces between the smartcard reader, the trusted component, and the monitor. The subsystem functionality is built into the trusted component, and resides within the trusted space. The subsystem 511 interfaces between the computer platform and smartcard, and the trusted component.

The subsystem is not critical for maintaining trust in the trusted component, in other implementations, the subsystem optionally can reside on the computer platform in the 'untrusted' computer platform space.

In a second implementation, trusted component 502 is accessed via the smartcard reader 103 and smartcard interface 305 via a software subsystem 511. The subsystem also provides an application interface function 512 for interfacing between applications 504 and the trusted component 502; and a verification application 513 for verifying via a third party accessed over the internet, or via a local area network/wide area network, integrity metrics data obtained by trusted component 502.

The trust placed in the computer entity by a user is composed of three separate parts;

- Trust placed in the user's trusted token device.
- The trust placed in the trusted component.

As described herein, levels or degrees of trust placed in the computer entity are determined as being relative to a level of trust which is placed in the trusted component and the smartcard. Although the amount of trust in a computer entity is related to many factors, a key factor in measuring that trust are the types, extent and regularity of integrity metrics checks which the trusted component

itself carries out on the computer entity, and the type, regularity and quality of the checks the smartcard makes on the trusted component.

Once the user has established by use of their smartcard that the trusted component is operating correctly, the trusted component is implicitly trusted. The trusted component is embedded as the root of any trust which is placed in the computing platform and the computing platform as a whole cannot be any more trusted than the amount of trust placed in the trusted component.

Although other computing entities can interact directly with a trusted component, by means of encrypted messages, to verify the operation of a trusted component, a human user operating a computing entity cannot directly interface with a trusted component, because the human user is a biological entity who is not capable of generating digital encrypted signals. The human user must rely on his visual and audio senses to verify the trustworthiness of a computing entity. The human user, in the general case, has no knowledge of the mechanisms at work inside the computing entity, and in the general case will be of an average level of education and sophistication, that is to say a normal average person.

The user is therefore provided with a trusted token in the form of a smartcard, in which the user may place a high degree of trust. The user's smartcard can interact with the trusted component of the computer entity in order to:

- Prove the identity of a trusted component to the user.

- Verify that the computer platform inside the computing entity is operating correctly, by virtue of integrity metrics measurement carried out on the computer platform by the trusted component.

Therefore, in the system of computing entities, there are chains of trust involved as follows:

- The user must trust the trusted token. This trust is based upon the reputation of the provider of the trusted token, who will typically be a corporation having access to the necessary technical and engineering resources to enable correct operation of the trusted token.

- Trust between the trusted token and trusted component. The trusted token smartcard must be able to verify correct operation of the trusted component using the smartcard.

- Trust in the computer platform. The trust in the computer platform derives from the monitoring of the computer platform by the trusted component, which is itself trusted.

Within this chain of trust, the link between the user and a computer entity can be viewed from the perspective of the user, the trusted platform which the user is using, and from the perspective of the trusted token (the smartcard), as described hereunder.

From the user's point-of-view, the user can only trust what s/he sees on the computer screen, and what s/he hears on the computer's audio output and/or printed output. The user is provided with a trusted token in the form of a smartcard which can be inserted into smartcard reader 103 of the computing entity. The smartcard carries out interactions using cryptographic messages and interrogations on behalf of the user. The smartcard is capable of initiating a request to the trusted component to perform integrity metrics, and is capable of denying authorization to application programs in the event that the smartcard

does not receive a satisfactory response to a request for verification from a trusted component.

In each specific implementation for carrying out the invention, the computing entity has a plurality of modes of operation.

Referring to Fig. 7 herein, there is illustrated a first mode of operation of a computer system comprising a computing entity and a smartcard under control of a user following a first process. In the process of Fig. 7, there is no application residing on the computing entity which requires use of the user's smartcard. The user is simply verifying the trustworthiness of the computing platform within the computer entity with the aid of the smartcard. In general, a user will wish to check the integrity of a computing entity as soon as the user logs on, and before the user performs any sensitive operations. The smartcard can be programmed to verify the integrity of the computing entity, via its trusted component, before the user carries out any other tasks using the computing entity. In step 700, a user inserts the smartcard into the smartcard reader of the computing entity which s/he is to use. In step 701, the user starts to use the graphical user interface of the computing platform. In step 702, a verification application 513 whose purpose is to enable a user having a smartcard to check the integrity of a trusted component of the computing entity and which is pre-loaded onto the computer platform, is activated by the user. Such activation may be by activating a pointing device, e.g. a mouse or track-ball which is visually placed over an icon displayed on a visual display of the computing entity. The verification interface 510 receives the commands from the graphical user interface for initiating a check of the trusted component by the smartcard and processes these into instructions in a form in which the smartcard can be instructed by the application to commence a verification process. In step 703, the interface sends a request signal to the smartcard requesting the smartcard to commence a verification operation on the trusted component. In step 704, the smartcard carries out integrity checks on the

trusted component. All communications between the smartcard and the trusted component are in encrypted format. The precise method by which the smartcard verifies the integrity of the trusted component is by a challenge-response integrity check method which is subject of a separate patent application by the applicants and is beyond the scope of this disclosure. In step 705 the smartcard, having completed the integrity check on the trusted component reports back to the user by displaying on the graphical user interface. The trusted component may report back to the user using the graphical user interface by a variety of methods, some of which are the subject of separate patent applications by the applicant, and which are outside the scope of this disclosure.

In one such method, the smartcard uses the trusted component to control the display on the monitor 100 to display information describing the computer platform, which has been determined by the trusted component, and in which an image specific to the smartcard is displayed on the visual display unit. For example, the smartcard may contain a difficult to recreate image data, preferably known only to the user. The trusted component may retrieve this image data from the smartcard and display it on the monitor, combined with other information describing integrity metrics and operation of the computer platform. Because the computing entity has no other way of obtaining the image data except from the user's smartcard, where it is pre-stored, and because the user can visually identify with a high degree of accuracy that the image is genuine, by visual inspection, the user then has confidence that the computing entity has in fact interacted with the smartcard (otherwise the image would not be obtainable).

Alternatively, in step 705, instead of the image data being displayed on the monitor of a computing entity which is being checked, the user may remove his smartcard from the smartcard reader, and insert the smartcard into his own palmtop device. The palmtop device is personal to the user, and therefore the user may trust the palmtop device to a higher extent than the computer entity.

The palmtop reader reads data from the smartcard verifying that the computer entity has passed the challenge-response tests made by the smartcard. The palmtop computer then displays to the user the information that the computer entity has passed the challenge-response test set by the smartcard. The user takes this as verification that the computing entity is trusted.

The above method operates where a user wishes to use a computing entity, and simply wishes to know whether the computing entity can be trusted.

Referring to Fig. 8 herein, there is illustrated schematically a second mode of operation in a case where an application resident on the computing entity, or resident on a remote computing entity with which the user wishes to communicate, requires that a user authorizes an operation, for example a commercial transaction operation.

The smartcard is configured by a system administrator, or smartcard service provider with details particular to the user. In step 800, the user inserts the smartcard into the smartcard reader of the computing entity. In step 801 the application or the operating system of the computing entity requests data from the smartcard. In step 803, the smartcard responds by sending a delay message to the computing entity, and requesting from the computing entity access to the computing entity's trusted component, so that the smartcard can verify the integrity of the computing entity. In step 804, the smartcard corresponds with the trusted component of the computing entity by means of integrity checks according to a challenge-response process as described herein above, to check the integrity of the computing entity. In step 805, if the smartcard determines that the integrity checks have been satisfied by the trusted component, the smartcard proceeds to respond to the request from the operating system or application for data for completing the operation.

The smartcard is programmed in such a way that the smartcard will never accept an interaction with an application, for example for the purposes of authentication, or to provide some cryptographic services, unless it can first verify the integrity of the computing entity to which it is connected by means of correspondence with a trusted component of the computing entity, in which the trusted component authenticates and checks integrity metrics of the computing platform. In this way, the user, who implicitly trusts the smartcard, is confident that his smartcard will only accept to be used by an application once it has verified that it is in a trusted environment. The smartcard does not need to explicitly report the results of the integrity checks to the user. The mere fact that an application has requested an interaction with a smartcard and that requested interaction has been satisfied is proof that the smartcard has been able to carry out this check and is satisfied with the result. Whether the smartcard accepts or rejects an interaction with an application is based upon pre-determined policies which are pre-programmed onto the smartcard by the smartcard issuer, or which can be configured by a user by programming the smartcard.

Configuration of the smartcard memory may be made by a user if this facility is provided by a smartcard vendor. For example a purchaser of a personal computer may be able to configure his own smartcard to operate according to user preferences. The smartcard may be pre-configured such that a user may be able to program the smartcard to interact with a computing entity in a Microsoft Windows ™ environment, even where a trusted component does not exist in a computing entity. A smartcard vendor may enable programming of a smartcard through a device such as a PDA palmtop computer. The precise configuration of the capabilities of each smartcard are specified by the smartcard provider as a design issue.

As another example, an internet service provider may provide a smartcard which only identifies itself correctly to the internet service provider, when it can

verify that the computing entity into which it is inserted, has passed various integrity checks specified by the smartcard. This provides protection for the internet service provider, to be able to confirm that a user will not connect to the internet service using an untrusted computer, which may be carrying viruses.

An advantage of the above two methods is that they do not require initiation by user interaction, but are initiated by the action of the smartcard being entered into the smartcard reader of a computer entity.

Referring to Fig. 9 herein, there will now be described one example of an operation of the computer entity during its interaction with a smartcard adapted as a trusted token. This example is based upon known technology according to the PCSC specification found in standard ISO 7816, and viewable at www.pcscworkgroup.com, which in the best mode is modified to allow initiation of commands from the smartcard.

Interaction between a smartcard and the trusted component allows the smartcard to authenticate the correct operation of the trusted component, and to obtain the trusted components response regarding integrity of the computer platform which the trusted component monitors. In a best mode implementation, the integrity verification process allows that the trusted component reports an interpreted result of a verification of correct operation of the computing entity to the smartcard. However in another mode of implementation the trusted component may not provide the mechanism to interpret the integrity measurements for the smartcard. In that case the smartcard must have access to a trusted third party server which provides this functionality.

Typically access to a trusted third party server by the smartcard will require the presence of a mechanism so that the smartcard can request such access to be provided by the computing entity.

Assuming you have a smartcard which can initiate a command to a trusted component, communicate with the trusted component for exchange of messages and information, send requests for information, receive results from the trusted component in response to those requests, and request access to third party server to be provided by the computing entity then integrity verification of the trusted component to the smartcard can be achieved. Implementation of initiation of user commands from a smartcard is known in "smartcards - from security tokens to intelligent adjuncts", by Boris Balacheff, Bruno Van Wilder, and David Chan published in CARDIS 1998 Proceedings.

Referring to Fig. 10 herein there is illustrated process steps carried out from a view point of the trusted component for verification of a computer platform in response to a request for a smartcard. In step 1000 the smartcard authenticates the trusted component as described herein before. In step 1001 the smartcard requests the trusted component to report on the integrity metrics of the computer platform, to the smartcard. In step 1002, the trusted component reports these to the smartcard. In step 1002, the trusted component may report back to the smartcard using the integrity metrics alone, for example a one way hash function of the BIOS of a processor of a computer platform which is transmitted to the smartcard. Integrity metrics can be checked by the smartcard in a relatively straight forward way in the best mode implementation, because the functionality exists within the trusted component to enable the trusted component to be requested to perform integrity metrics and verify the integrity metrics of an associated computer platform to a third party requesting those integrity metrics. This is the most basic form.

Referring to Fig. 11 herein, there is illustrated schematically a system of computer apparatus comprising a computing entity 1100 comprising a computer

platform and a monitoring component as described herein before; a trusted token device 1101 capable of communicating with computing entity 1100; and a remote server 1102 capable of carrying out data processing functionality. The remote server 1102, also comprises a second computing platform and second monitoring component. In use, the remote server 1102 may be managed by a reliable service provider, for example an internet service provider, in which a user of a trusted token device may have a degree of trust established through, for example, a contractual relationship with the internet service provider, such as subscribing to a service provided by the internet service provider.

Referring to Fig. 12 herein, there is illustrated schematically a fourth mode of operation of a token device and a computing entity within the system of computers illustrated in Fig. 11. In the fourth mode of operation, a monitoring component (trusted component) within the computing entity 1100 is requested by the smartcard 1101 to provide a set of data checks on the computer platform within the computing entity 1100. Trusted token device 1101 may not have a sufficiently high data processing capability to carry out data processing on data supplied by the computer entity 1100. Therefore, the computer entity sends the integrity metrics data to a remote server 1102 trusted by smartcard, which verifies that the integrity metrics data supplied by the monitoring component is correct by comparing this with a set of expected integrity metrics. The expected integrity metrics may be either supplied by the monitoring component itself, from pre-stored data within that component, or where the computer platform is of a common type, the trusted server 1102 may store sets of expected integrity metrics for that type of computer platform. In either case, the trusted server 1102 performs the heavy computational data processing required for verification of the integrity metrics with the expected integrity metrics, and digitally signs the result of this verification.

Received 15-Dec-99 21:41 From-44 114 268 0931 To-THE PATENT OFFICE Page 05

Depending upon how the token device is pre-programmed and the amount of data processing capability resident on the trusted token device, there are two modes of operation.

In step 1200, the trusted token authenticates the trusted component as described herein before. In step 1201 the smartcard requests the trusted component to verify the integrity metrics of the computer platform, and to report back to the smartcard. In step 1202, the trusted component, having available the integrity metrics data as part of its ongoing monitoring of the computer platform, sends the integrity metrics data to the smartcard, along with a set of certified expected integrity metrics for that computer platform. In step 1203, the smartcard sends the received integrity metrics data and the certified expected integrity metrics data to the trusted third party server for computation. This message also includes an identification of the smartcard device itself. Sending of the integrity metrics data and expected integrity metrics data from the smartcard to the trusted server is via the computer entity itself, which routes the data, for example over the internet, to the remote trusted server 1102. In step 1204, the server processes the integrity metrics data, and verifies that the certified expected integrity metrics are currently certified, and compares it with the expected integrity metrics data received from the smartcard. This is a heavy computational step, for which the trusted server is suited to. In step 1205, having compared the integrity metrics data with the expected integrity metrics data, the server may then send a verification data back to the smartcard via the computer entity. The verification data may comprise a digital signature of the server. In step 1206, the smartcard receives the verification data comprising a data signature and either accepts or rejects that digital signature as being valid, and therefore the verification data.

Referring to Fig. 13 herein, there is illustrated schematically process steps carried out in a fifth mode of operation of the smartcard and computing entity of Fig. 11, whereby the computing entity delivers the results of a verification of a set

Received 15-Dec-99 21:41 From-44 114 268 0931 To-THE PATENT OFFICE Page 06

of integrity metrics data along with a digital signature, to the smartcard, certifying a set of integrity metrics data which is also supplied to the smartcard.

Referring to Fig. 13, in step 1300 the smartcard authenticates the trusted component as described herein above. In step 1301, the smartcard sends a request message to the trusted component requesting verification of integrity metrics of the computer platform, and reports back to the smartcard. In step 1102, the trusted component sends the set of measured integrity metrics of the computer platform to a third party (the trusted component either knows which third party server will be trusted by the smartcard or the smartcard needs to specify which third party server should be used), together with a trusted components own digital signature, and receives from the third party server the result of the verification of these integrity metrics and together with a digital signature. This is, as a result of step 1303 of the third party server comparing the set of integrity metrics received from the trusted component with its own stored set or a retrieved set of expected integrity metrics for the type of computer platform identified by the trusted component and adding the digital signature in step 1304. In step 1305, the trusted component, having received the digital signature sends the set of integrity metrics, together with the digital signature to the smartcard.

The above examples of Figs. 11 to 13 is of operation of the best mode implementation, in which the trusted component performs integrity metrics monitoring.

From the perspective of the smartcard, any application which interacts with the smartcard, either a graphical user interface, or another application, must be aware of the fact that the smartcard may request an interaction with a trusted component of a platform. In the case where the smartcard will require to interact with a third party computing entity the application which interacts with the

Received 15-Dec-98 21:41 From-44 114 268 0931 To-THE PATENT OFFICE Page 07

smartcard must also allow the smartcard to interact with a network server. But the best mode implementation, the smartcard should be able to request access to integrity verification data of a computer platform independently from the application to which it is talking to on a computer entity.

Upon receiving a request from an application of a computing entity to use a functionality of the smartcard, for example to authorize a transaction, the smartcard may initiate a request for the monitoring component to supply monitoring information on the trustworthiness of the state of the computer platform. Communication between the smartcard and the trusted component is by way of a protocol module resident on the computer platform which is responsible for communications between the computing entity and the smartcard token device. When an application on the PC requires access to the smartcard, the protocol stack handles these communications. The computing entity can therefore filter commands which come from the card and are independent from the computing entity application such as checking the integrity of the computer platform, and can accommodate commands which come from the smartcard. From the point of view of the application, interactions of the smartcard with other resources on the computing entity are transparent. This can be done using the technology in "smartcards - from security tokens to intelligent adjuncts", by Boris Balacheff, Bruno Van Wilder, and David Chan published in CARDIS 1998 Proceedings merged with PCSC technology.

Referring to Fig. 14 herein, there is illustrated schematically an operation to verify the trustworthiness of a computing entity, as viewed from a perspective of the smartcard. In step 1400, the smartcard is inserted into the smartcard reader and contacts 604 on a smartcard connect with corresponding contacts in the smartcard reader. (This can also be done using contactless technology). In step 1401 the smartcard receives a request from the graphical user interface, via the subsystem 511, to check the trustworthiness of the platform. This signal is

generated by the graphical user interface in response to keystroke inputs and/or pointing device inputs from a user. Alternatively, in step 1402, the smartcard may receive a request for access to functionality generated by an application either resident on the local computing entity, or resident on a remote computing entity. In step 1403, the smartcard initiates a request for communication with a trusted component, in response to the signals received from steps 1401 or 1402. In step 1404, the smartcard then receives integrity metrics data from the trusted component (via the subsystem 511 in the first implementation, and directly in the best mode implementation). In step 1405, the smartcard, having received integrity metrics data from the trusted component needs to check the integrity metrics data against the certified integrity metrics data that it would be able to trust the platform. The smartcard sends the integrity metrics data to a trusted server external of the computing entity. The smartcard sends the integrity metrics data back to the subsystem 511, (or the trusted component itself in the best mode) which then routes the integrity metrics data to an address provided by either the trusted component or the smartcard, of a trusted third party server. The trusted third party server performs checks with certified expected integrity metrics in step 1406 and generates a result message and digitally signs it. In step 1407, the trusted server sends the results message and digital signature back to the smartcard via the computing entity, and in step 1408, the smartcard receives the result message and digital signature data from the trusted server. The third party server may be a publicly accessible device. The smartcard is able to verify the digital signature to authenticate the third party server and can then use the result of the verification of the integrity metrics.

Ideally, the server is bound with the smartcard, for example both the server and the smartcard are issued by the same vendor, or body, for example an internet service provider.

Received 15-Dec-99 21:41 From-44 114 268 0931 To-THE PATENT OFFICE Page 09

For example, where the smartcard is provided by an internet service provider, and the smartcard is unable to authenticate the trustworthiness of a computing entity, then the internet service provider may either refuse to communicate with the computing entity, or may provide a limited set of functionality, such as those available to the general public, to the computing entity, rather than a full set of services available only to registered subscribers.

Having provided the trusted component, in one specific implementation according to the present invention, the remaining elements of the smartcard and the application communicating with each other may be provided by a modification to the convention applications. In this implementation, a conventional smartcard may be used, which is pre-programmed to respond to a poll signal from an application to initiate a request to a trusted component to perform integrity metrics checks.

Referring to Fig. 15 herein, there is illustrated schematically elements of a possible first generation implementation of a system according to the present invention. Fig. 15 shows a logical view of components of first generation implementation. A trusted component 1500 comprises a processor and memory physically separated from a computer platform and resident in a trusted logical space as herein before described. The computer platform comprises a further processor and data storage means and is resident in a computer platform space 1501. Subsystem 1502 and applications 1503 reside in the computer space 1501. Subsystem 1502 contains an application interface 1503, a verification application 1504, and a smartcard interface 1505. The smartcard interface communicates with smartcard reader 1506 which is also in the computer platform space 1501, which accepts smartcard 1507. The application interface 1503, contains the PCIA stack.

Received 15-Dec-99 21:41 From-44 114 268 0931 To-THE PATENT OFFICE Page 10

Referring to Fig. 16 herein, there is illustrated schematically a method of operation of the first generation implementation of Fig. 15 herein, for smartcard 1507 interacting with the trusted component prior to giving a functionality 'X' in response to a request for functionality 'X' from an application. In this method of operation, calls to the PCSC stack could be done through the PCIA stack in order to provide the PCIA functionality transparently. In the best mode, the PCSC stack would incorporate the PCIA stack and functionality. In step 1600 the application sends the request for functionality 'X' to the smartcard via the PCSC stack resident in the application interface 1503 in the subsystem 1502. In step 1601, the PCSC stack sends a command to the smartcard, requesting functionality 'X' from smartcard. In step 1602 the smartcard responds with a request for verification of the trustworthiness of the computing entity, which is received by the PCSC stack. In step 1603, the PCSC stack receives the request; through PCIA functionality the message will be sent to the trusted component. Either by using the separate PCIA stack or through existing PCIA functionality the message is sent to the trusted component to initiate the integrity checks. This may be sent directly from the application interface 1503 to the trusted component 1500. In the first specific implementation the verification application 1504 and the subsystem 1502 is used by the trusted component to perform the integrity metrics checks. In a best mode implementation, the trusted component 1500 contains functionality within itself to perform these integrity checks on the computer platform directly. In step 1506, the trusted component (in conjunction with the verification application in the first implementation all by itself in the best mode) sends the result of the integrity verification with a digital signature and certificate data to the smartcard. In step 1607 the smartcard receives the result of the integrity verification with the digital signature, verifies the digital signature to authenticate the trusted component, and if satisfied, it trusts the result of the verification of integrity. Based on this result it then decides whether or not to provide the application with functionality "X". The application can then proceed. The smartcard has verified the trustworthiness of the computer platform by requesting to perform an integrity

challenge on the computing entity's trusted component and only once satisfied about the result of this challenge accepts to provide functionality to the application.

Received 15-Dec-99 21:41 From-44 114 268 0831 To-THE PATENT OFFICE Page 12

Claims

1. A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

2. The system as claimed in claim 1, wherein said token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

3. The system as claimed in claim 1, further comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

4. The system as claimed in claim 3, wherein said monitoring component sends a detailed integrity response to a third party server if requested to do so in said integrity challenge.

5. The system as claimed in claim 1, wherein said monitoring component reports a detailed integrity response to said token device and said token device sends said integrity response to said third party server if it requires the third party server to help interpret said detailed integrity response.

6. The system as claimed in claim 1, in which a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

7. The system as claimed in claim 1. wherein a third party server sends a simplified integrity response to said token device.

8. The system as claimed in claim 1, operating to add a digital signature data to said simplified integrity response, said digital signature authenticating said third party server to said token device.

9. The system as claimed in claim 1, wherein said monitoring component sends a detailed integrity response to said third party server.

10. The system as claimed in any one of the above claims, in which said token device is requested to take an action.

11. The system as claimed in any one of the above claims in which said token device requests to take an action.

12. The system as claimed in any one of the above claims in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data.

Received 15-Dec-99 21:41 From-44 114 268 0831 To-THE PATENT OFFICE Page 14

13. The system as claimed in claim 1, wherein said monitoring component is capable of establishing an identity of itself.

14. The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device.

15. The system as claimed in claim 1, wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

16. The system as claimed in claim 1, wherein a said specific action comprises authorising said computing platform to undertake a transaction on behalf of a user of said system.

17. A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein said token device sends an integrity challenge to said monitoring component;

said monitoring component generates a response to said integrity challenge;

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and

said computer platform displays said verification data on a visual display screen.

18. A computing entity comprising:

a computing platform having a first data processor and first data storage means;

a monitoring component having a second data processor and second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself.

interface means for communicating with a token device, said interface means communicating with said monitoring component,

wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

19. The computing entity as claimed in claim 18, wherein on communication between said token device and said interface means, said

monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

20. The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component.

21. The computing entity as claimed in claim 18, wherein said interface means comprises said computer platform.

22. The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0.

23. The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means.

24. The computing entity as claimed in claim 18, wherein said interface means is configured to send and receive data according to a pro-active protocol.

25. A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and

said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

26. A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform; and

said monitoring component being able to report a set of certified reference data together with said data checks.

27. The method as claimed in claim 25, wherein said certified reference data includes a set of metrics to be expected when measuring particular components of said computing platform, and includes digital signature data identifying an entity that certifies said reference data.

28. The method as claimed in claim 25, wherein said step of reporting verification of said monitoring operation comprises sending a confirmation signal to a token device said confirmation signal describing a result of said monitoring operation.

29. The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token device external of said computing entity.

Received 15-Dec-98 21:41 From-44 114 268 0831 To-THE PATENT OFFICE Page 18

30. The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data.

31. The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said monitoring component; and

transmitting said result message and said digital signature data from said interface.

32. A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a token device;

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component;

in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation;

by receipt of a satisfactory said result message, said token device offers said functionality to said application.

Received 15-Dec-99 21:41 From-44 114 268 0831 To-THE PATENT OFFICE Page 18

33. The method as claimed in claim 32, wherein said monitoring component sends a detailed integrity response to a third party server if requested in an integrity challenge by said token device.

34. The method as claimed in claim 32, wherein said monitoring component reports a detailed integrity response to said token device, and said token device sends said integrity response to a third party server if it requires the third party server to help interpret said detailed integrity response.

35. The method as claimed in claim 32, wherein a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

36. The method as claimed in claim 32, wherein a third party server sends a simplified integrity response to said token device.

37. The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a third party server to said token device.

38. A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means, and a monitoring component comprising a second processor and second memory means, by means of a token device, said token device comprising a third data processor and a third memory means, said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform;

said token device receiving a poll signal from said computer platform;

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

39. A token device for verifying a status of a computing entity, said token device comprising:

a data storage device; and

means for communicating with a computing entity;

wherein said data storage device is configured to store a status request message for requesting a status data from said computing entity.

40. The token device as claimed in claim 39, further comprising a data processor.

41. The token device as claimed in claim 39, said device being configured to be responsive to a poll signal operating in accordance with PC/SC specification 1.0, said token device being capable of initiating a command to be handled by a software stack on the computer entity, in response to said poll signal according to said poll signal according to a proactive protocol.

42. A method of verifying a status of a computing entity, by means of a token device provided external of said computing entity, said method comprising the steps of:

said token device receiving a poll signal;

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity; and

said token device receiving a result message, said result message describing the result of said verification.

43. A method by which a token device can obtain verification of a state of a computing platform by using a monitoring component,

said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself , and establishing a report of said at least one data check; and

wherein said token device has data processing capability and behaves in an expected manner;

said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability

wherein , said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform.

44. A token device comprising a data processor and a memory device, said token device configured to perform at least one data processing or signaling function:

wherein said token device operates to:

receive an integrity check data from an external source;

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function; and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function.

Received 15-Dec-99 21:41 From-44 114 268 0831 To-THE PATENT OFFICE Page 23

Abstract

SMARTCARD USER INTERFACE FOR TRUSTED COMPUTING PLATFORM

There is disclosed a trusted computer entity which can be used as a stand-alone device, or as a node in a network of connected computing entities, e.g. as an internet port, the computing entity having a trusted monitoring component which monitors operation of a computer platform, wherein a user is provided with a smartcard trusted token by means of which the user can establish confidence in the computer platform by means of the smartcard communicating with the trusted component and the trusted component verifying to the smartcard that the computer platform is operating correctly. A user may be issued with a plurality of smartcards, and the smartcards may be capable of verifying a level of trust of any one of a plurality of computing entities equipped with a trusted component.

Fig. 5

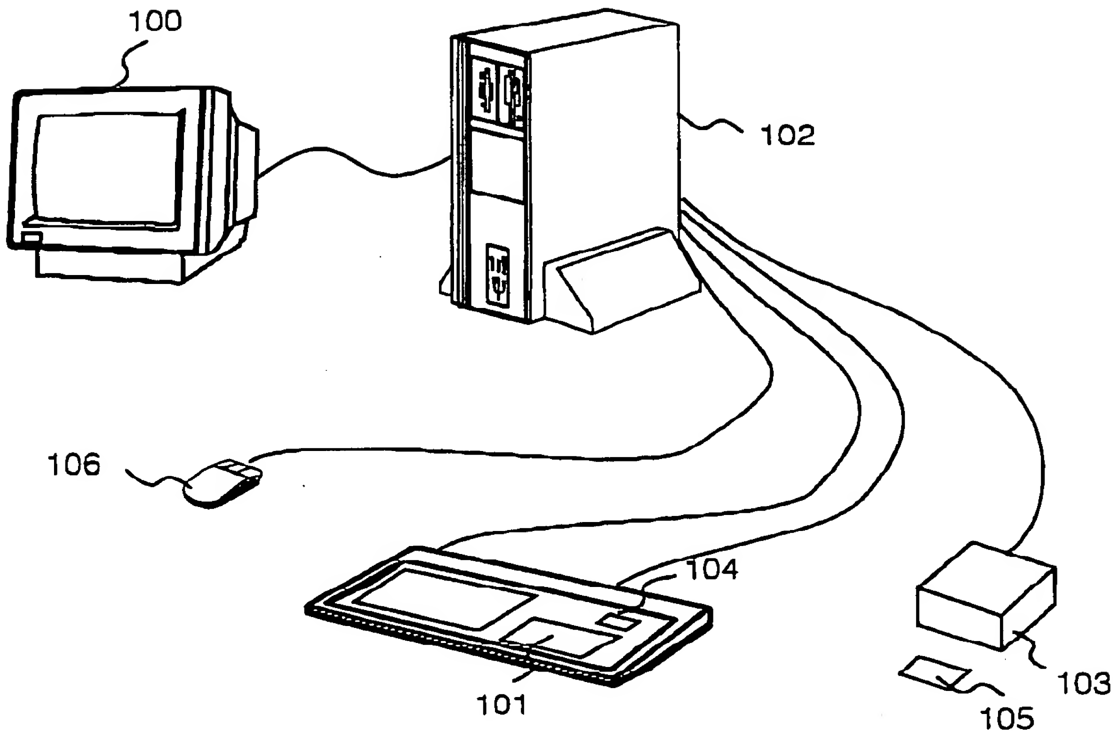


Fig. 1

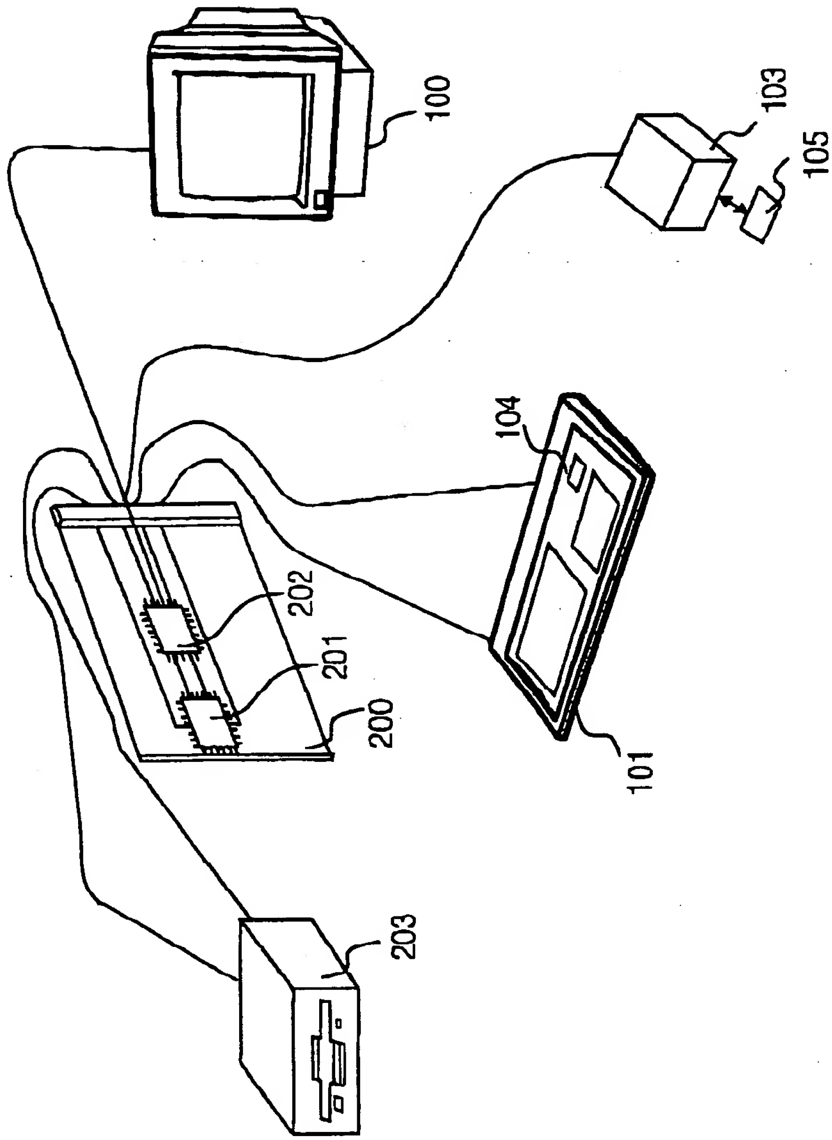
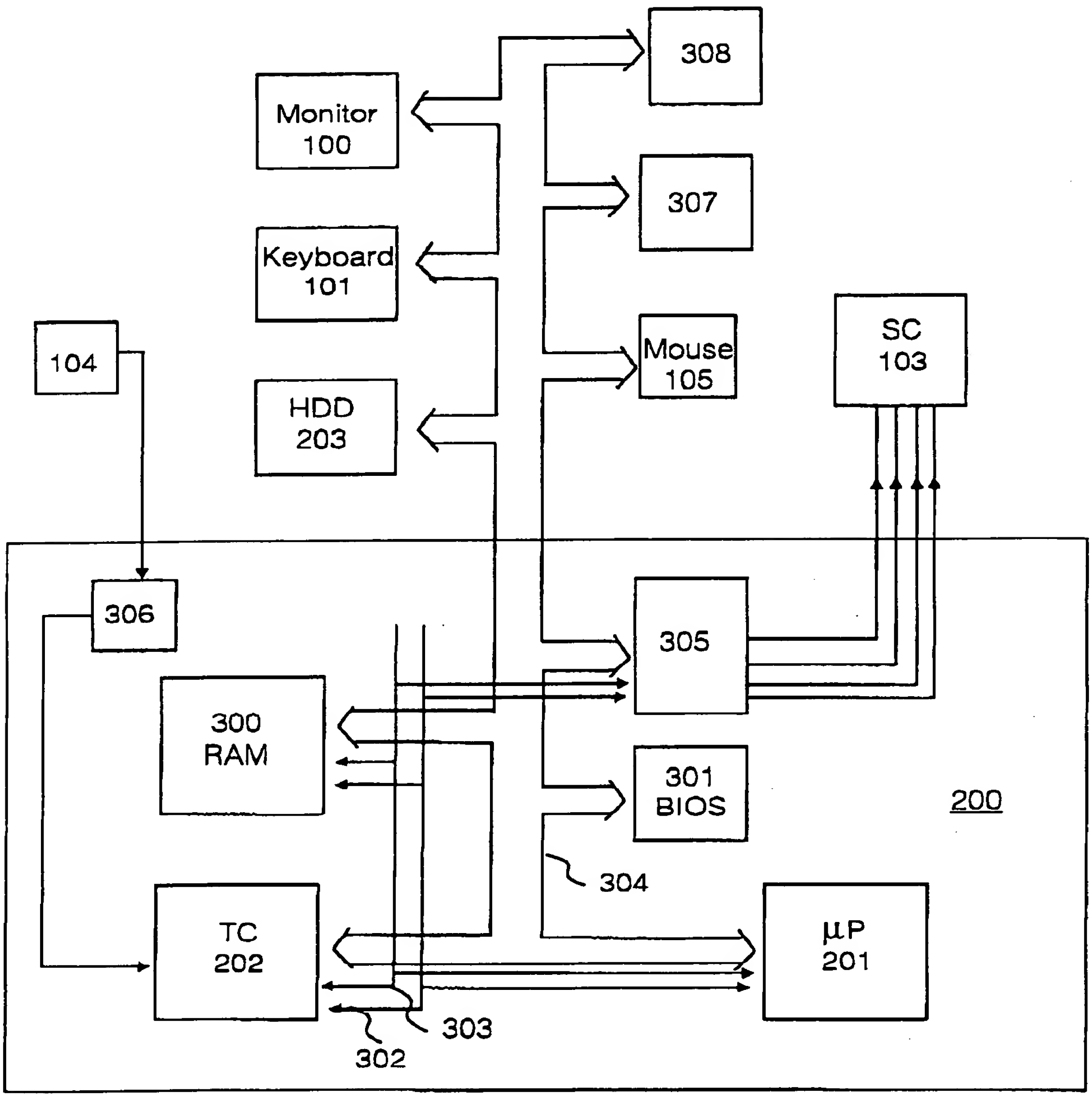


Fig. 2



308
Monitor
100
307
Keyboard
101
SC
103
104
Mouse
105
HDD
203
306
305
300
RAM
301
BIOS
200
304
TC
202
µP
201
303
302

Fig. 3

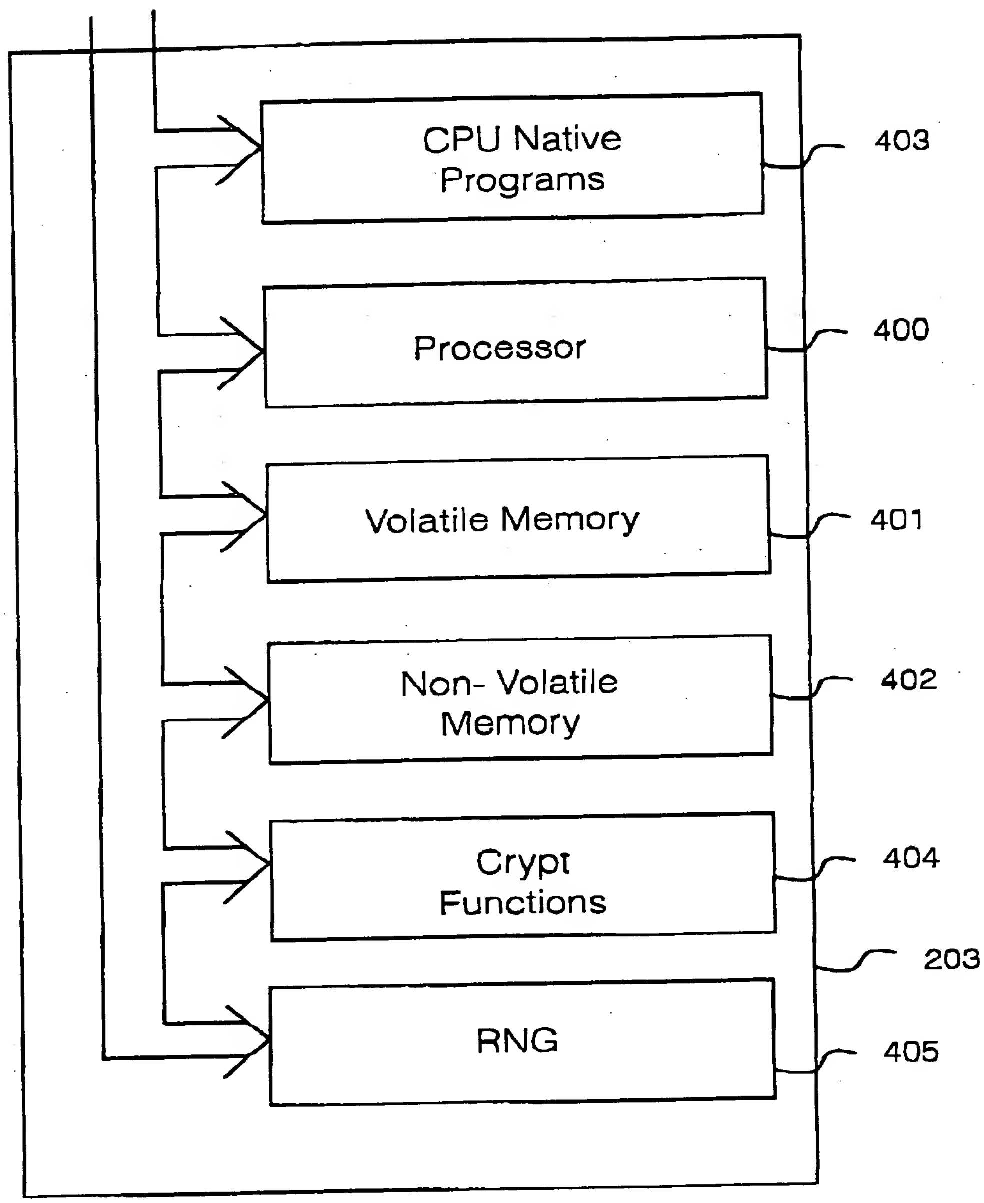

CPU Native Programs
403
Processor
400
Volatile Memory
401
Non- Volatile Memory
402
Crypt Functions
404
203
RNG
405

Fig. 4

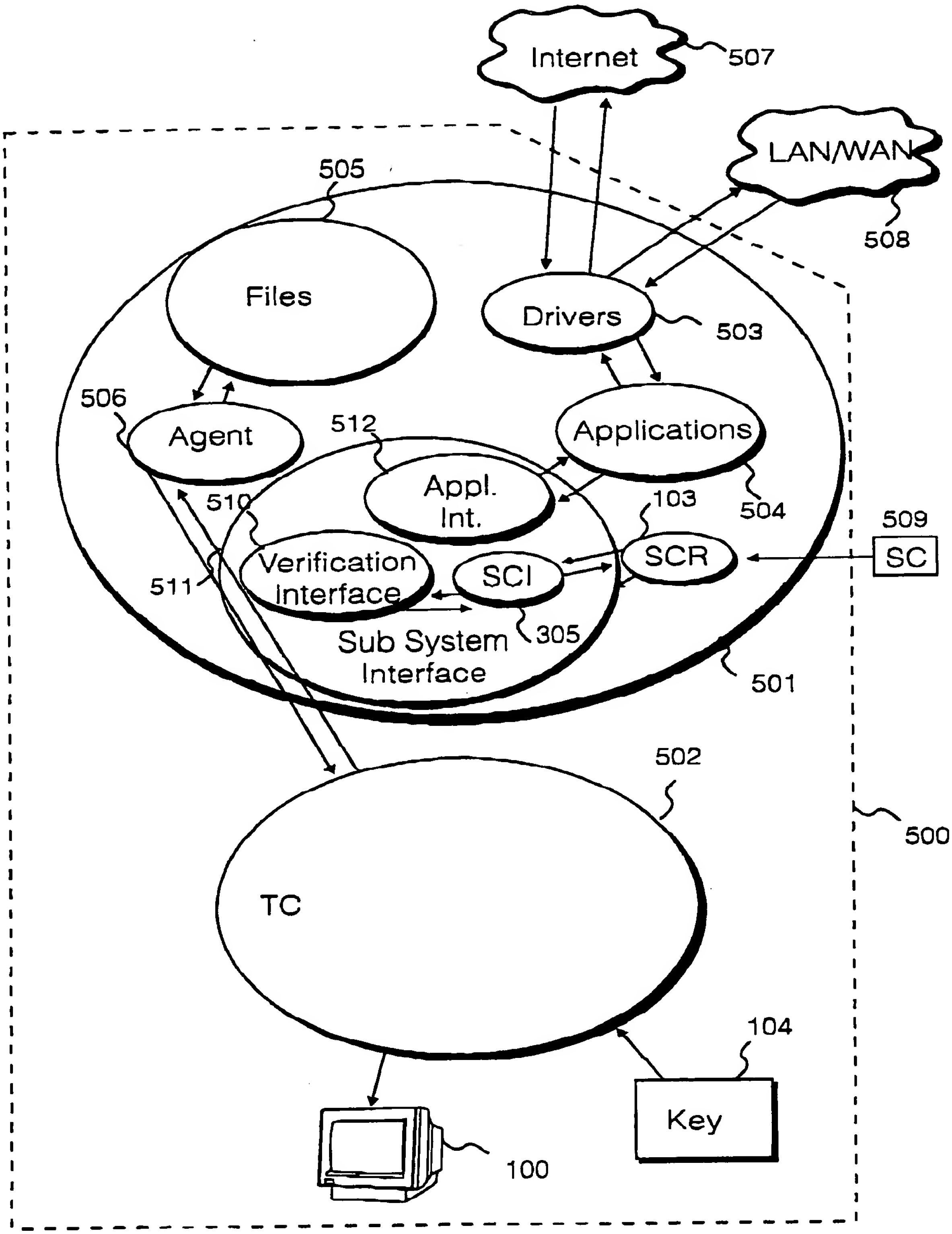


Fig. 5

Received 15-12-99 21:50 From-44 114 268 0931 To-THE PATENT OFFICE Page 09

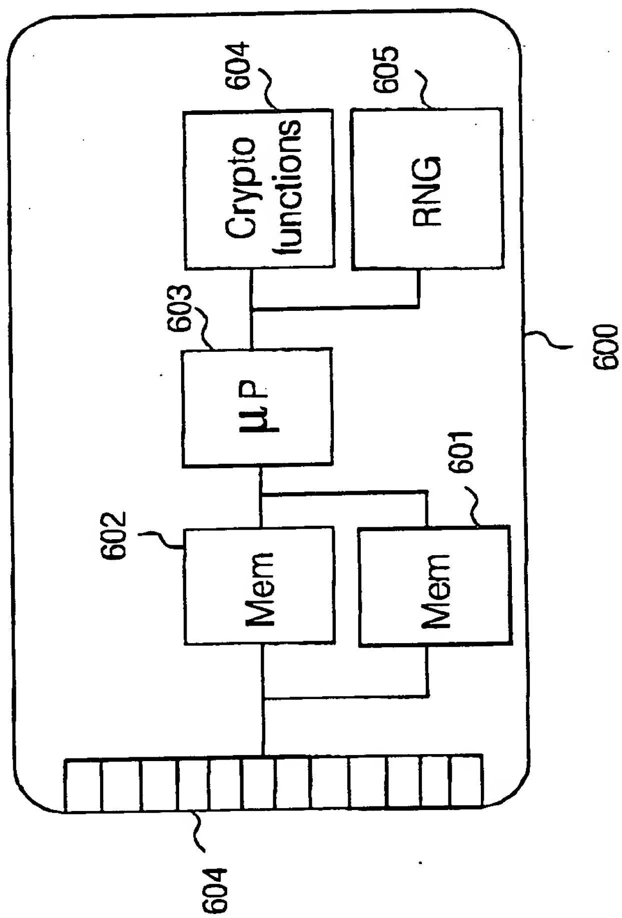


Fig. 6

Received 15-12-99 21:50 From-44 114 268 0931 To-THE PATENT OFFICE Page 10

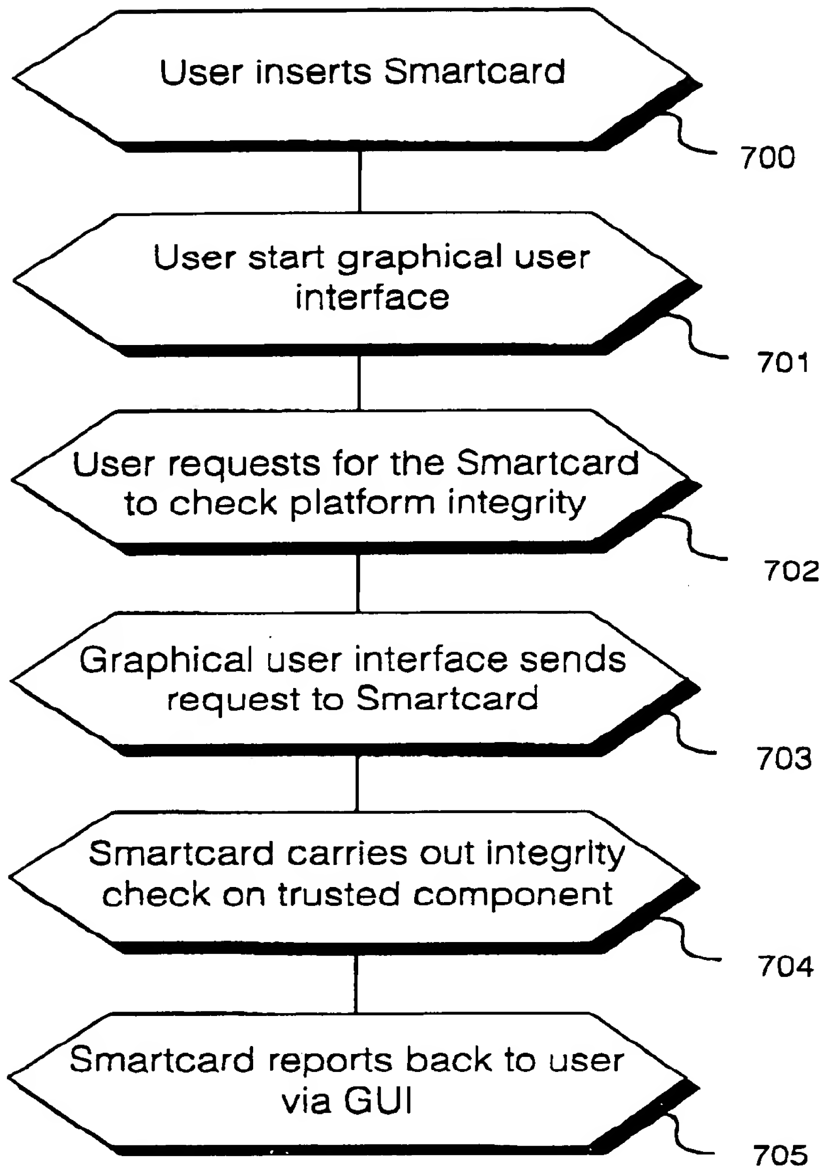


Fig. 7

Received 15-12-98 21:50 From-44 114 268 0931 To-THE PATENT OFFICE Page 11

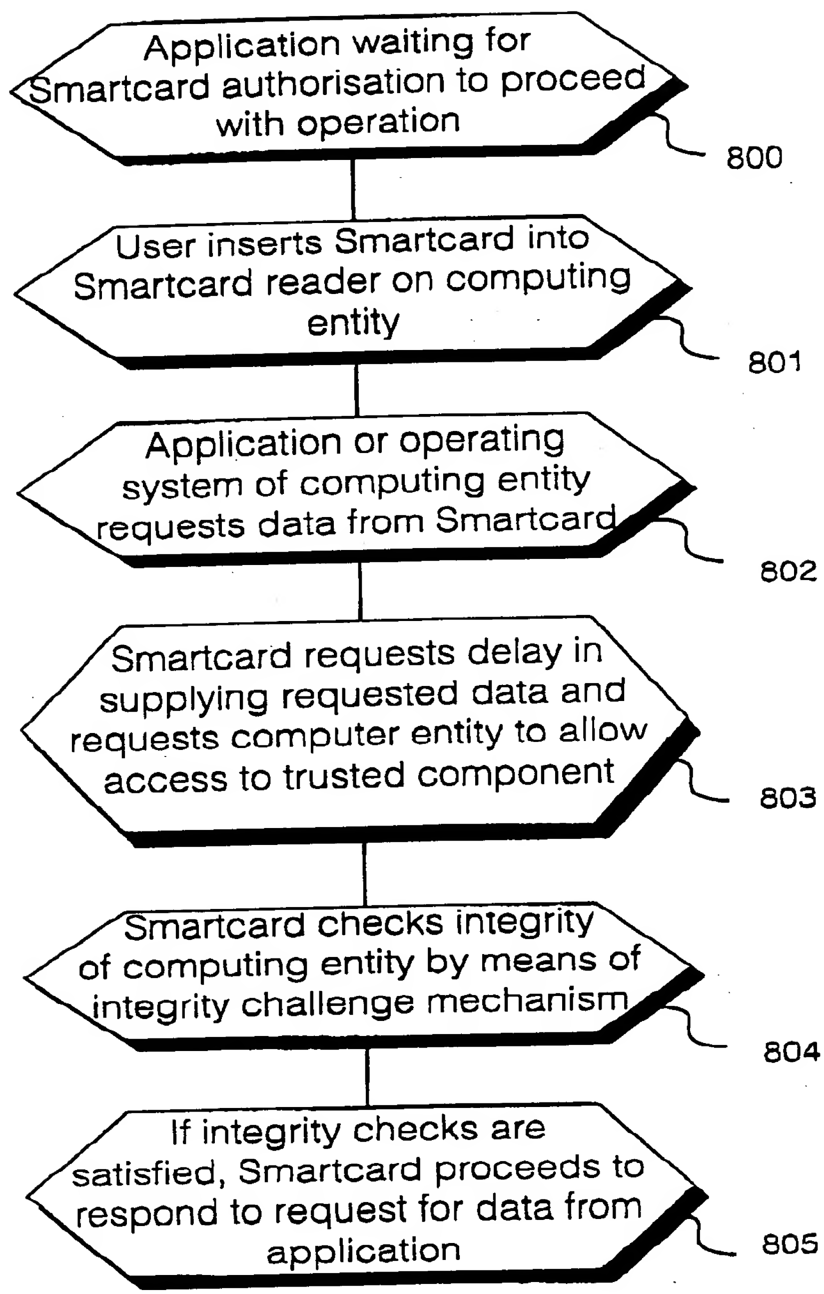


Fig. 8

Received 15-12-99 21:50 From-44 114 268 0831 To-THE PATENT OFFICE Page 12

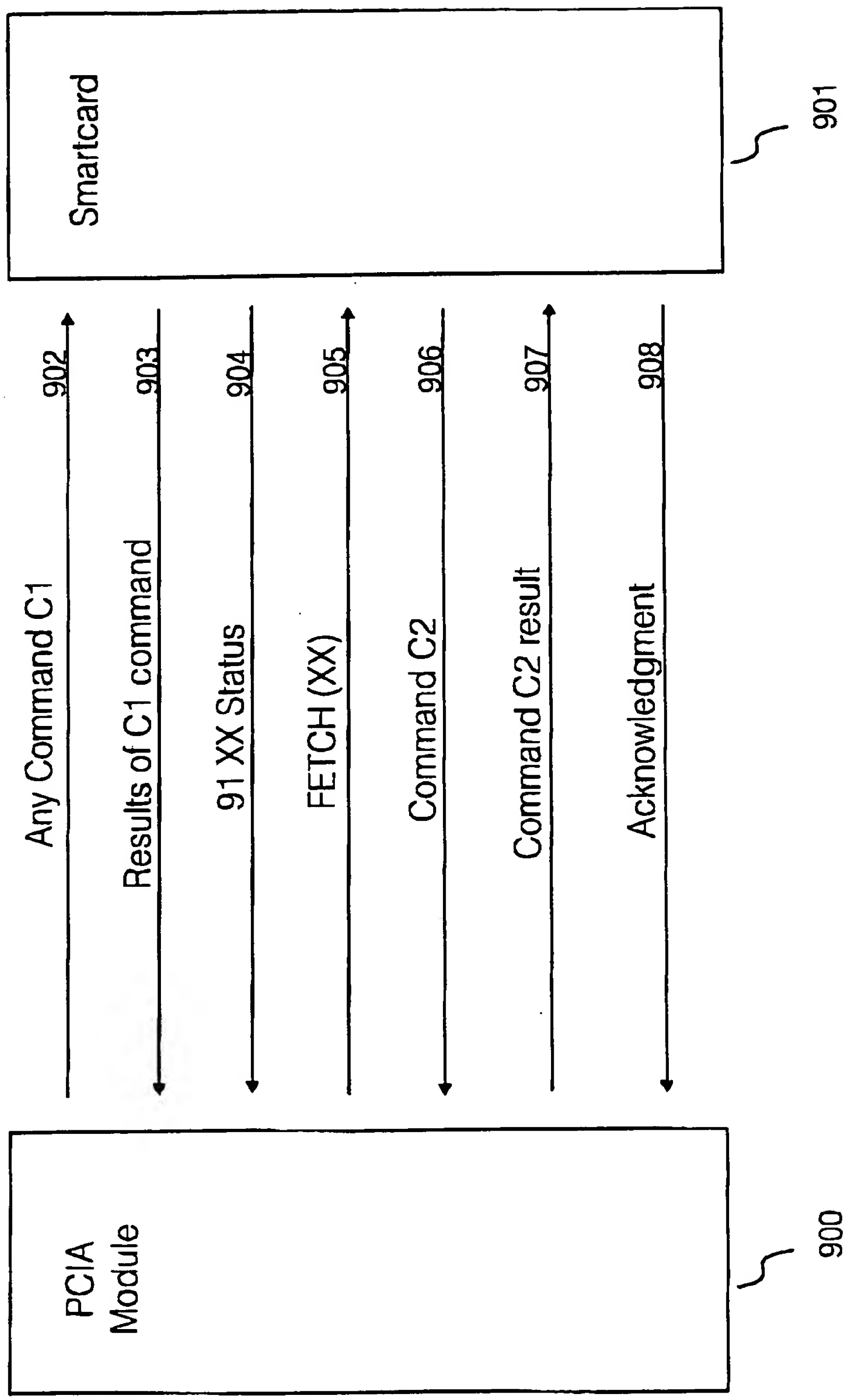

Smartcard
901
Any Command C1
902
Results of C1 command
903
91 XX Status
904
FETCH (XX)
905
Command C2
906
Command C2 result
907
Acknowledgment
908
PCIA Module
900

Fig. 9

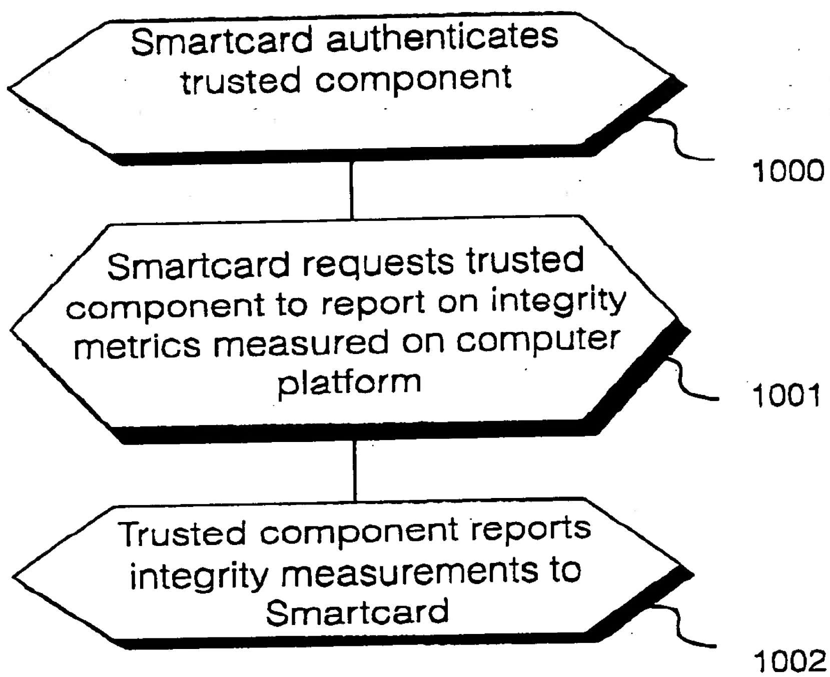


Fig. 10

Received 15-12-99 21:50 From-44 114 268 0831 To-THE PATENT OFFICE Page 14

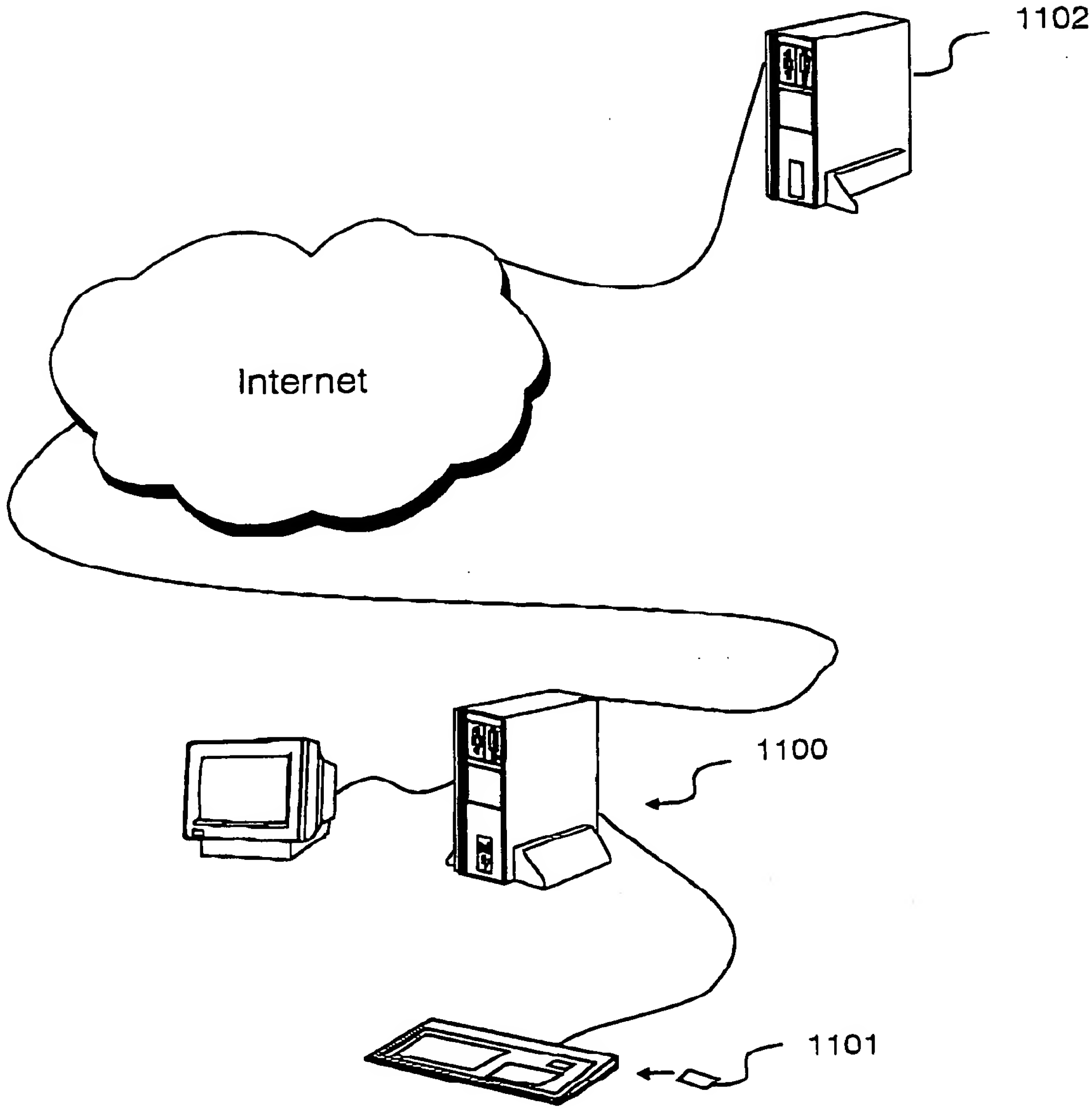


Fig. 11

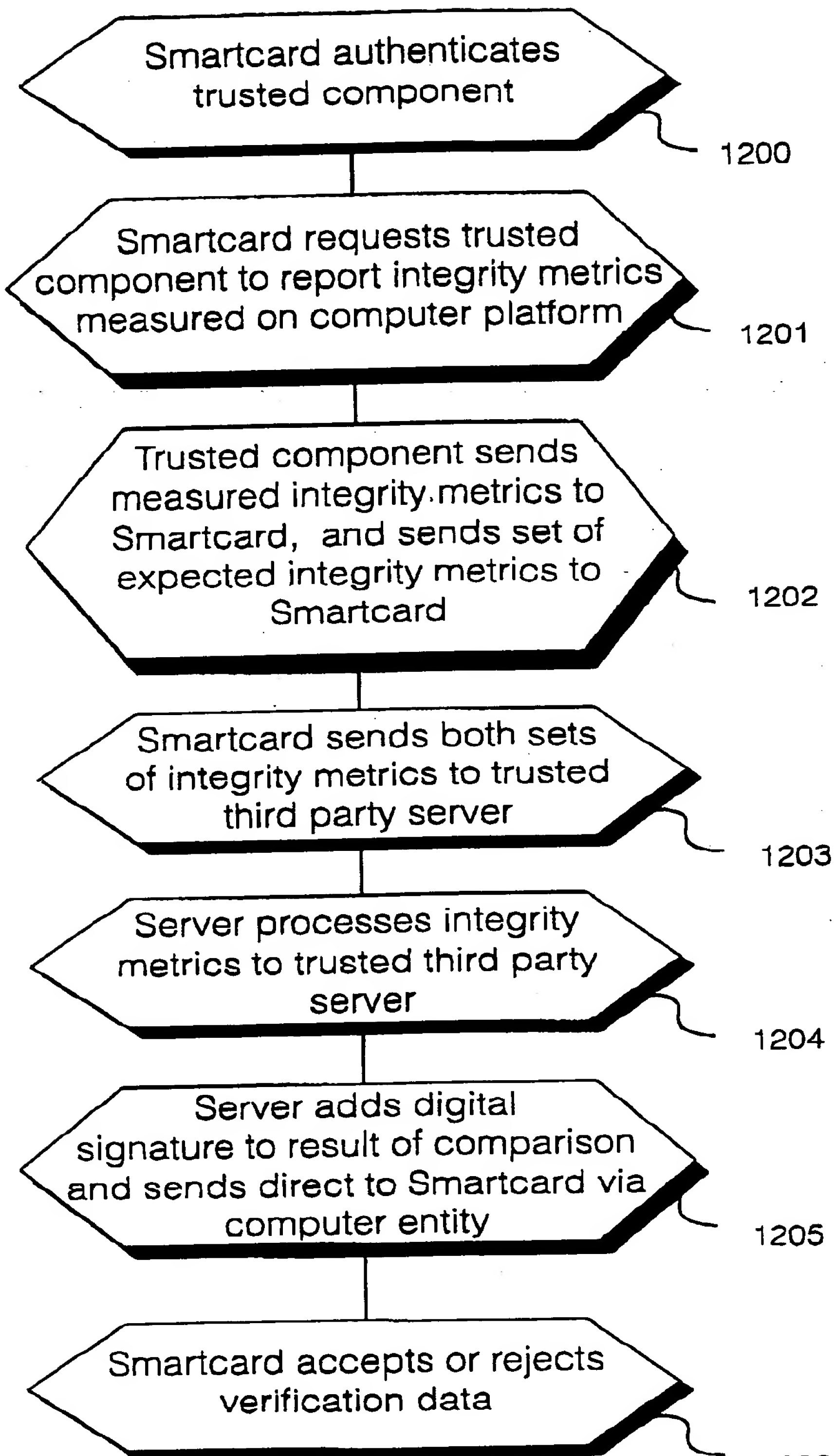

Smartcard authenticates trusted component
1200
Smartcard requests trusted component to report integrity metrics measured on computer platform
1201
Trusted component sends measured integrity metrics to Smartcard, and sends set of expected integrity metrics to Smartcard
1202
Smartcard sends both sets of integrity metrics to trusted third party server
1203
Server processes integrity metrics to trusted third party server
1204
Server adds digital signature to result of comparison and sends direct to Smartcard via computer entity
1205
Smartcard accepts or rejects verification data
1206

Fig. 12

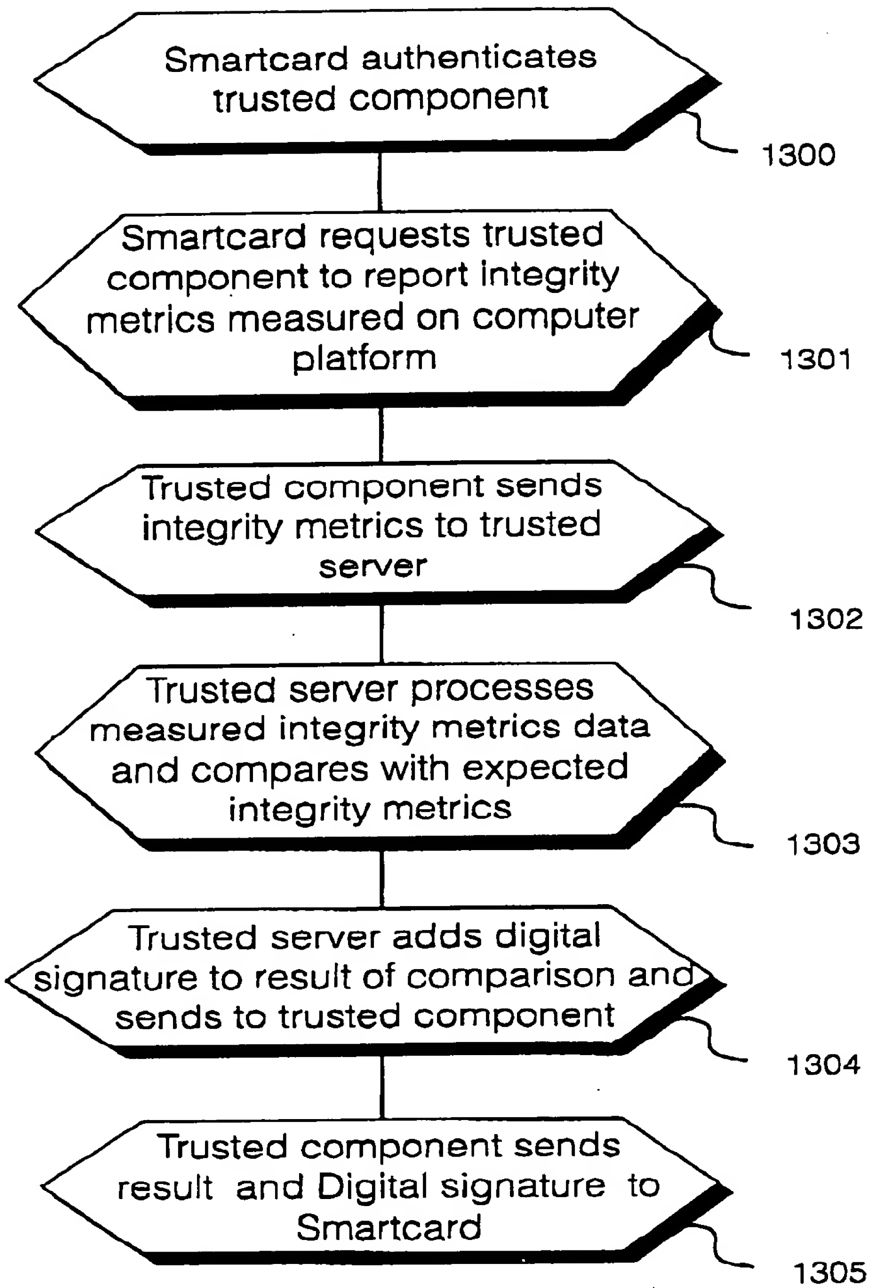

Smartcard authenticates trusted component
1300
Smartcard requests trusted component to report integrity metrics measured on computer platform
1301
Trusted component sends integrity metrics to trusted server
1302
Trusted server processes measured integrity metrics data and compares with expected integrity metrics
1303
Trusted server adds digital signature to result of comparison and sends to trusted component
1304
Trusted component sends result and Digital signature to Smartcard
1305

Fig. 13

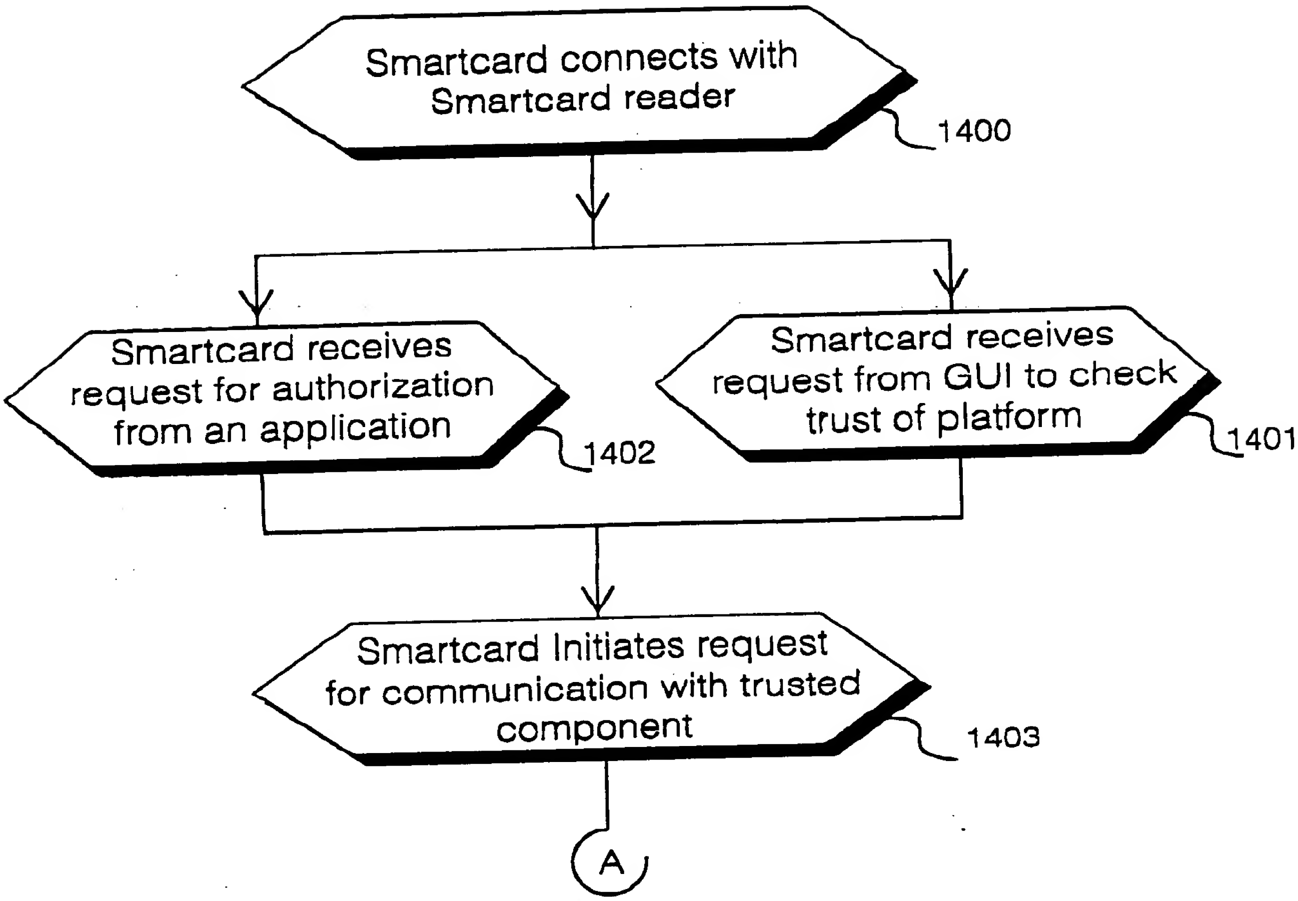


Fig. 14

Received 15-12-99 21:50 From-44 114 268 0931 To-THE PATENT OFFICE Page 18

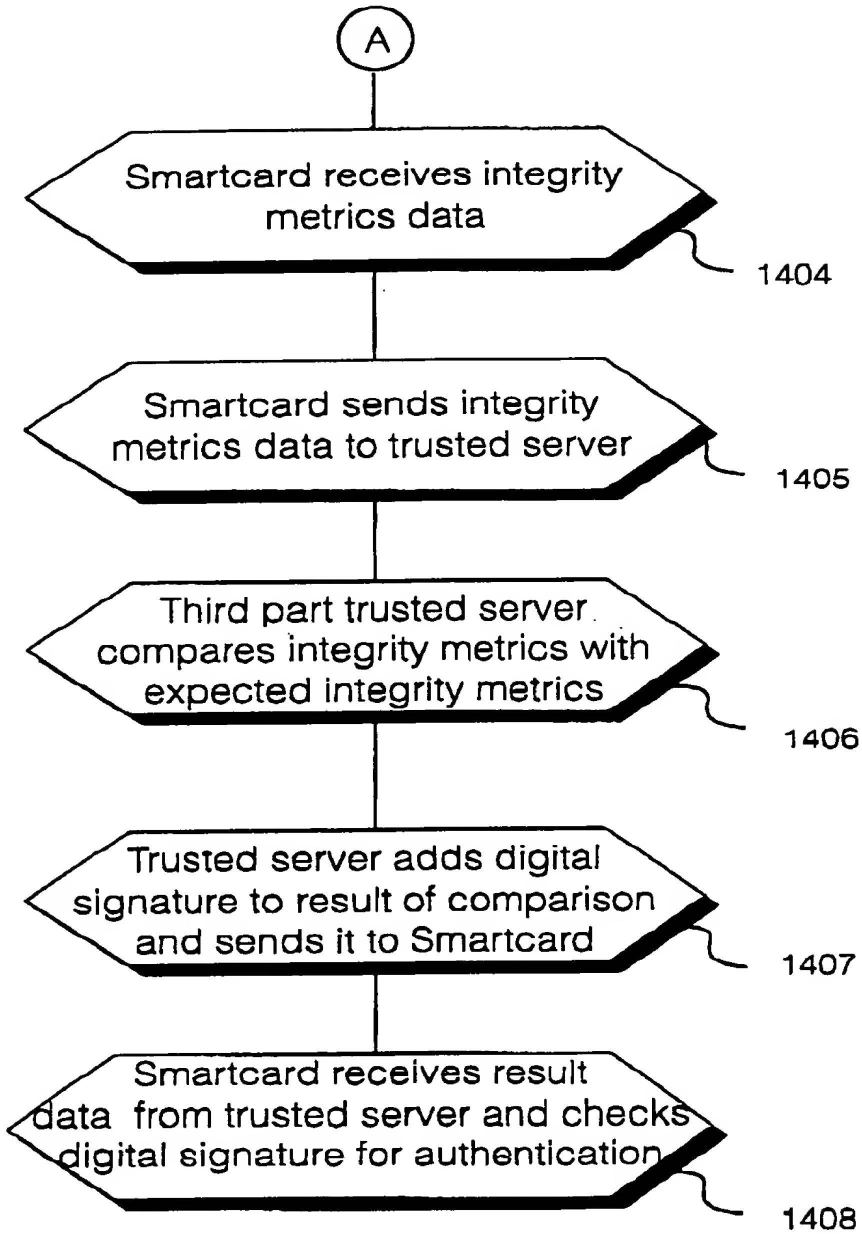

A
Smartcard receives integrity metrics data
1404
Smartcard sends integrity metrics data to trusted server
1405
Third part trusted server compares integrity metrics with expected integrity metrics
1406
Trusted server adds digital signature to result of comparison and sends it to Smartcard
1407
Smartcard receives result data from trusted server and checks digital signature for authentication
1408

Fig. 14b

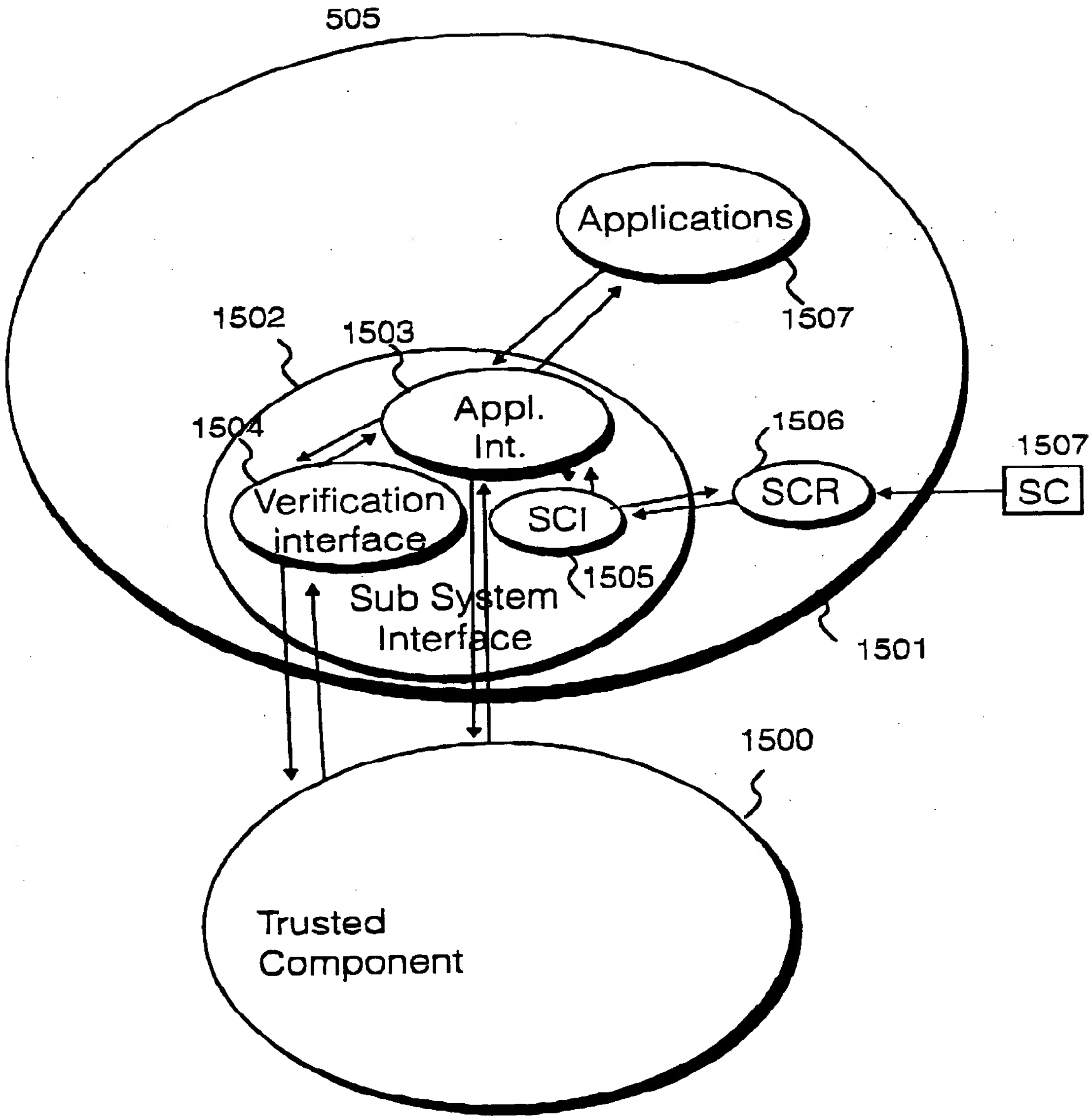

505
Applications
1507
1502
1503
Appl.
Int.
1504
Verification
interface
SCI
1506
SCR
1507
SC
1505
Sub System
Interface
1501
1500
Trusted
Component

Fig. 15

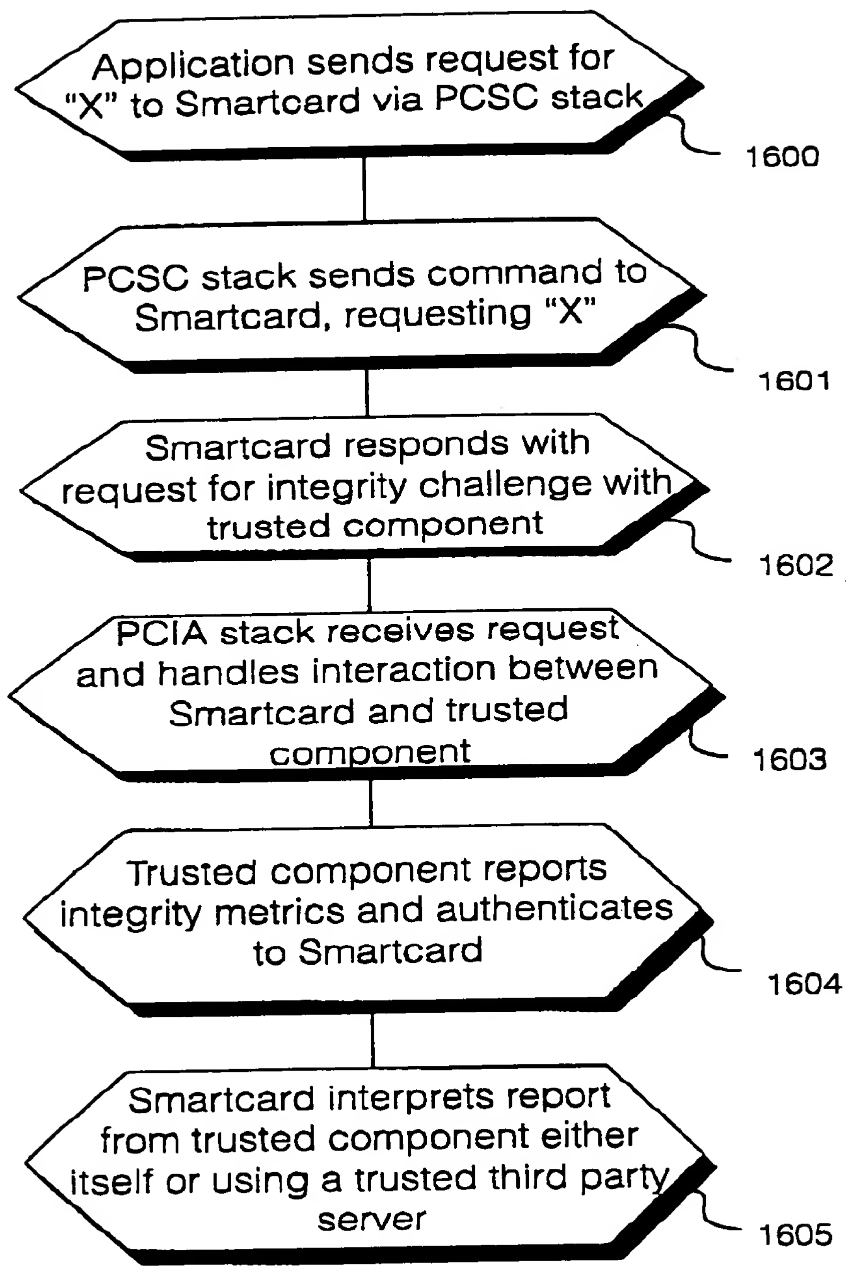

Application sends request for "X" to Smartcard via PCSC stack
1600
PCSC stack sends command to Smartcard, requesting "X"
1601
Smartcard responds with request for integrity challenge with trusted component
1602
PCIA stack receives request and handles interaction between Smartcard and trusted component
1603
Trusted component reports integrity metrics and authenticates to Smartcard
1604
Smartcard interprets report from trusted component either itself or using a trusted third party server
1605

Fig. 16

This Page Blank (uspto)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☑ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☑ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** ______________________________

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)